العنوان:	الإشكاليات القانونية لحماية سلامة المعلومات : دراسة تطبيقية على الحماية الجنائية من الإتلاف المعلوماتي
المصدر:	مجلة الفكر الشرطي - مركز بحوث الشرطة - القيادة العامة لشرطة الشارقة - الإمارات
المؤلف الرئيسي:	القطري، محمد نصر محمد عمض
المجلد/العدد:	مج24, ع93
محكمة:	نعم
التاريخ الميلادي:	2015
الشهر:	أبريل
الصفحات:	133 - 181
رقم MD:	683672
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	المعلومات، أمن المعلومات، اتلاف المعلومات، الجرائم المعلوماتية، الحماية الجنائية
رابط:	http://search.mandumah.com/Record/683672

الإشكاليات القانونية لحماية سلامة المعلومات

دراسة تطبيقية على الحماية الجنائية من الإتلاف المعلوماتي[1]

DOI: 10.12816/0011423

الدكتور. محمد نصر محمد عوض القطري[2]
أستاذ مشارك القانون العام - أكاديمية القاهرة الجديدة - مصر

مستخلص

لقد شهد العالم اليوم ثورة هائلة في مجال تقنية المعلومات ولا تكاد نجد مؤسسة تعليمية أو غير تعليمية إلا ولها اتصال وارتباط بهذه التقنية، بل حتى على مستوى الأفراد. ومع التطور الهائل في هذا المجال، كان لا بد من بيان الأحكام المتصلة بهذه التقنيات استخداماً وتعاقداً، وآثاراً وحقوقاً. وحيث إنّ الإتلاف المعلوماتي ليس قاصرا على الإتلاف المادي للنظام المعلوماتي، ولكن قد يتعلق بإتلاف معلومات وبرامج النظام المعلوماتي التي يعتمد عليها في قيامه بعمله وأدائه لوظائفه المختلفة ويقع الإتلاف المعلوماتي من خلال وسائل تقنية وفنية من خلال معلومة أيضا ولكنها معلومة مدمرة ومتلفة لغيرها من المعلومات وذلك من خلال ما يعرف بالفيروسات. وتكمن المشكلة في الإتلاف المعلوماتي أن طرقه لا تدخل تحت حصر، كما أن الحماية الجنائية الموضوعية قد لا تشمل كافة الصور، ومنها استخدام الفيروسات كأسلوب تقني للإتلاف المعلوماتي وهي "استخدام وصناعة ونشر الفيروسات وهي أكثر جرائم الإنترنت انتشارا وتأثيرا. لذلك فقد تناول ماهية الإتلافات للبرامج أو المعلومات وحكمها ثم محل جرائم الإتلاف المادي والإتلاف المعلوماتي ثم تعرض البحث للإتلاف العمدي للبيانات ثم اختتمت الدراسة بالحماية غير المباشرة من الإتلاف المعلوماتي. وانتهى البحث إلى ضرورة تجريم الولوج في النظام المعلوماتي في حد ذاته وهو ما يطلق عليه الحماية غير المباشرة للمعلومات وليس فقط الاكتفاء بتجريم فعل الإتلاف، كما أوصت الدراسة بضرورة تشديد العقوبات حال ارتكاب جريمة الإتلاف المعلوماتي أو حتى مجرد الولوج إلى نظم المعالجة المعلوماتية والعمل على المساواة في ذلك بين الاعتداء على الجهات الحكومية أو الاعتداء على الجهات الخاصة كما أوصت الدراسة بالمساواة في العقوبة بين الجريمة العمدية وغير العمدية وبخاصة على المعلومات المودعة في بنوك المعلومات، وأن يتم إفراد قانون خاص لتجريم كافة صور الاعتداء على المعلوماتية، وأن يتم عقد الاتفاقات الدولية الثنائية للتسليم في جرائم الإتلاف المعلوماتي.

مفردات البحث:

الإتلاف المعلوماتي — تقنية المعلومات — جرائم الإنترنت — الفيروسات — النظام المعلوماتي— الإتلاف المادي— سلامة المعلومات — إتلاف البرامج — المعالجة الآلية للبيانات.

1- ورد هذا البحث للدورية بتاريخ أكتوبر 2012 وقيد تحت رقم 2015/6 (2012/10/83)، وأحيل للتحكيم في يناير 2013 وأجيز للنشر في يوليو 2014.

2- حصل الدكتور محمد نصر على درجة الدكتوراه في القانون الدولي الجنائي من جامعة المنصورة عام 2008 وهو عضو في الجمعية المصرية للاقتصاد السياسي والتشريع والجمعية المصرية للقانون الدولي واتحاد المحامين الأفروآسيوي وعضو جمعية الصداقة المصرية السودانية وعضو جمعية سيدات الأعمال العرب وهو يعمل محاضرًا في أكاديمية القاهرة الجديدة قسم القانون الدولي وقسم القانون الجنائي وحصل على العديد من درجات الشرف وشهادات التقدير ودروع التميز وقام بإنتاج عدة بحوث وكتب منشورة كما شارك في العديد من الندوات والمؤتمرات.

Information Protection's Legal Problems
A study Applied on Criminal Protection against Information Destruction [1]

DOI: 10.12816/0011423

Dr. Mohammed Nasr Mohammed Awad Al Qatri [2]
Associate Professor of Public Law – New Cairo Academy – Egypt

Abstract:

Nowadays, world is witnessing an enormous IT revolution both in the level of institutions and individuals, and because of this stupendous progress, it was incumbent upon us to explain rules governing use of this technology, contracting via it as well as impacts of such technology and related rights. Information destruction is not just limited to the physical destruction of information system but rather the destruction of information system's information and programs. Information can be destructed by technological and technical means or even by destructive information (viruses). Study urges that criminal protection doesn't cover all forms of information destruction like the use and industry of viruses, the most serious and prevalent form of cybercrimes. Research turns spotlight on the destruction of programs and information in addition to setting related rules. Research also deals with deliberate destruction of data, and concludes with indirect protection of information. In its recommendations, the research stresses the necessity for toughening the penalty of information destruction, or even data processing. Study doesn't draw a distinction between destruction of government institutions and private ones' information: it treats destruction equally in both cases and requires the same toughened penalty, and the same thing, according to the study, applies to intentional and unintentional destruction of information stored in information banks. Among the recommendations of the study is also the conclusion of bilateral international extradition agreements in information destruction crimes.

Keywords:

Information Destruction – IT – Internet Crimes – Viruses – Information System – Physical Destruction – Information Safety – Programs Destruction – Automatic Data Processing.

1-**Manuscript:** was submitted in October 2012 under No 6\2015, refereed in January 2013.

2-**Biography:** Dr. Mohammed obtained his doctorate degree in International Criminal Law from Mansoura University in 2008. He is member of Egyptian Association for Political Economy and Egyptian Association for International Law as well as member of Afro - Asian Lawyers Federation. He is moreover member of Sudanese Egyptian Friendship Association. He is a lecturer at New Cairo Academy, International and Criminal Law sections. He has been awarded a host of appreciation certificates and titles and published numerous books and researches. He has taken part in a great deal of conferences and symposia.

مقدمة :

لقد شهد العالم اليوم ثورة هائلة في مجال تقنية المعلومات ولا تكاد تجد مؤسسة تعليمية أو غير تعليمية إلا ولها اتصال وارتباط بهذه التقنية، بل حتى على مستوى الأفراد. ومع التطور الهائل في هذا المجال، كان لا بد من بيان الحكم الشرعي لهذه التقنيات (استخداماً وتعاقداً، وآثاراً وحقوقاً وغير ذلك).

ولأنّ الإتلاف المعلوماتي ليس قاصرا على الإتلاف المادي للنظام المعلوماتي، فإنّه قد يتعلق بإتلاف معلومات وبرامج النظام المعلوماتي التي يعتمد عليها في قيامه بعمله وأدائه لوظائفه المختلفة ويقع الإتلاف المعلومات من خلال وسائل تقنية وفنية من خلال معلومة أيضا ولكنها معلومة مدمرة ومتلفه لغيرها من المعلومات وذلك من خلال ما يعرف بالفيروسات. وتكمن المشكلة في الإتلاف المعلوماتي أن طرقه لا تدخل تحت حصر، كما أن الحماية الجنائية الموضوعية قد لا تشمل كافة الصور، ومنها استخدام الفيروسات كأسلوب تقني للإتلاف المعلوماتي وهي "استخدام وصناعة ونشر الفيروسات وهي أكثر جرائم الإنترنت انتشارا وتأثيرا.

أهمية البحث :

لم يعد الإتلاف قاصرا على ما كان يقع على الأموال المادية بل الظهور مع تطور الحياة وانتقالها إلى معلومات، ومحاولة إتلافها وهو الأمر الذي يؤثر على الاستفادة منها ويهدر قيمتها. ولم يعرف المشرع المصري الإتلاف المعلوماتي في القانون الجنائي Sabotage information ويعرف اتجاه في الفقه الإتلاف المعلوماتي بأنه إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ولا يهدف التدمير إلى مجرد الحصول على منفعة من الحاسب الآلي أيا كان شكلها سواء الاستيلاء على أموال أو الإطلاع على معلومات ولكن إحداث الضرر بالنظام المعلوماتي وإعاقته عن أداء وظيفته[1]. وفي اتجاه آخر هو

1- LUCAS (A.): Le droit de l'informatique P.U.F. 1987.P.519. By.E.M: le financement de logiciels.GAZ.pal.1985.p.396

مقدمة في الحاسب الآلي وتقنية المعلومات، طارق بن عبد الله الشدي، دار الوطن للنشر بالرياض الطبعة الثانية، وانظر مدخل إلى الإنترنت وتكنولوجيا الحاسب الشخصي – د/ خالد الطويل و د/ عبد الرحمن

"محو المعلومات أو البرامج كلية أو تدميرها إلكترونيا أو أن يتم تشويه المعلومات أو البرامج على نحو فيه إتلاف بها يجعلها غير صالحة للاستعمال".

مشكلة البحث :

الإتلاف المعلوماتي ليس فقط إتلافا ماديا لماديات النظام المعلوماتي، ولكن يتعلق بإتلاف معلومات وبرامج النظام المعلوماتي التي يعتمد عليها في قيامه بعمله وأدائه لوظائفه المختلفة[1] ويقع الإتلاف المعلوماتي من خلال وسائل تقنية وفنية من خلال معلومة أيضا ولكنها معلومة مدمرة ومتلفة لغيرها من المعلومات وذلك من خلال ما يعرف بالفيروسات[2].

العلي والأستاذ / نزار مبروكة – الدار العربية للعلوم – الطبعة الأولى – عام 1420هـ. موقف الشريعة الإسلامية من جرائم الحاسب الآلي والإنترنت، عطا عبد العاطي محمد السنباطي دار النهضة العربية، القاهرة، الطبعة الأولى، 1422هـ، ص33. الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، د/ عبد الفتاح بيومي حجازي، دار الكتب القانونية، مصر، 2002م، ص68. الحماية الجنائية الخاصة – دراسة مقارنة – د/ أسامة قايد، دار النهضة العربية، القاهرة، عام 1994م، ص41. انظر: الحماية الجنائية للتجارة الإلكترونية، د/ مدحت عبدالحليم رمضان، دار النهضة العربية، القاهرة عام 2001م، ص102. الحكومة الإلكترونية – مسرح الجريمة –، د/ عبد القادر الفنتوخ، جريدة الرياض، العدد: 12312، الأحد 26/ 12 / 1422هـ، ص41.

1- د. على عبد القادر القهوجي – الحماية الجنائية للبيانات المعالجة إلكترونيا – بحث مقدم لمؤتمرات القانون والكومبيوتر والإنترنت – كلية والقانون الإمارات العربية المتحدة – 2000، ص19 د. هشام فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط، طـ1994، ص134 د. عمر الوقاد – الحماية الجنائية للمعلومات – مجلة روح القوانين – حقوق طنطا – إبريل 1998 ص52، د. عوض محمد – دراسات في الفقة الجنائي الإسلامي – دار المطبوعات الجامعية – الإسكندرية 1998، ص 91.

2- الحماية الجنائية للبيانات المعالجة إلكترونياً، د/ علي بن عبد القادر القهوجي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، عام2000م. الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني، د/ هدى حامد قشقوش، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، عام 2000م، ص13.

وتكمن المشكلة في الإتلاف المعلوماتي أن طرقه لا تدخل تحت حصر، كما أن الحماية الجنائية الموضوعية قد لا تشمل كافة الصور، ومنها استخدام الفيروسات كأسلوب تقني للإتلاف المعلوماتي وهي "استخدام وصناعة ونشر الفيروسات وهي أكثر جرائم الإنترنت انتشارا وتأثيرا"[1]، وتعد الخسائر التي تسببها جرائم نشر الفيروسات، والتي تضر بالأفراد والشركات، وبخاصة الشركات الكبيرة منها حيث ينتج عنها توقف بعض الأعمال نتيجة إتلاف قواعد بيانتها، وقد يصل الضرر في بعض المنشآت التجارية، وعلى سبيل المثال وصلت الأضرار المادية لفيرس الحب الشهير إلى (7.8) مليون دولار، واستمر انتشار الفيروس لخمسة أشهر منه (55) نوعا. وبخاصة بعد استخدام هذه الوسائل (الفيروسات المعلوماتية) في حماية بعض البرامج الأصلية، من البرامج التي يتم الحصول عليها كبرامج مقلدة منتهكين الحماية المقررة للملكية الفكرية.

منهجية البحث:

اتبعت المنهج الاستقرائي التحليلي لمعرفة ماهية الفيروس المعلوماتي وطريقة عمله، لإحداث جريمة الإتلاف المعلوماتي، وإمكانية الجمع بين الحماية الموضوعية المباشرة، والتجريم غير المباشر لمجرد الولوج في الأنظمة الخاصة بالمعلمات وبخاصة لبنوك المعلومات العامة أو الخاصة[2].

فكرة الحماية الجنائية لبرامج الحاسب الآلي، للدكتور/ محمد محمد شتا، دار الجامعة الجديدة للنشر الإسكندرية، 2001م، ص22. د. عزة محمود خليل – المرجع السابق – ص 253.

1- كما هو معلوم أن الفيروسات الإلكترونية ليست وليدة إنشاء الشبكة العنكبوتية فهي موجودة منذ الأربعينات راجع د. إياس الماجري – جرائم الإنترنت – 1422 هـ – 2002 – ص 90.

2- Arabian computer news , Vol. 61 , no.3 march 1989.pp.10-11.

وهى إحدى أنواع البرامج المخصصة للتعامل مع الحاسب الآلي، والتي تتكون من مجموعة من الأوامر، إلا أن تلك الأوامر المكتوبة في هذه البرامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكن عند كتابة كلمة أو أمر ما أو حتى بمجرد فتح البرنامج الحامل للفيروس أو الرسالة البريدية المرسل معها الفيروس فيؤدي إلى تلف الجهاز، أو قيام الفيرس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به وقد عرفها اتجاه في الفقه بأنها نوع من البرامج التي تؤثر في البرامج الأخرى بحيث تعدل في تلك البرامج لتصبح نسخة منها، وهذا يعني ببساطة أن الفيروس ينسخ نفسه من حاسب آلي إلى

خطة البحث:

عرضنا في البحث ماهية الإتلاف للبرامج أو المعلومات في المبحث الأول، ثم لمحل جرائم الإتلاف المادي والإتلاف المعلوماتي في المبحث الثاني، ثم تعرضنا للإتلاف العمدي للبيانات في المبحث الثالث، ثم تعرضنا للحماية غير المباشرة من الإتلاف المعلوماتي في المبحث الرابع.

المبحث الأول
ماهية إتلاف البرامج أو المعلومات

لقد حدثت في العالم اليوم تغيرات عدة، يأتي من أبرزها إدخال واستخدام الحاسب الآلي في أغلب شؤون الحياة، وبخاصة في الأسواق المالية والتجارية، حيث تتجه الشركات العالمية في التجارة الدولية بشكل واضح نحو الاستفادة من الحاسبات الآلية وغيرها، لأداء العديد من الوظائف في مجال العمل التجاري كحفظ المعلومات ومتابعة الإنتاج والمخزون ومراقبة النواحي المالية، وسنعرض لأهم الأخطار التي تواجه هذا التطور والمتمثل في الجرائم التي تستخدم البيئة المعلوماتية، أو التي تستهدفها.

وفيه مطلبين:

المطلب الأول: المقصود بإتلاف البرامج والمعلومات.

المطلب الثاني: إتلاف البرامج والمعلومات ببرامج فيروسية.

حاسب آلي آخر بحيث يتكاثر بأعداد كبيرة. وفي اتجاه آخر بأنه برنامج يصممه بعض المجرمين لأهداف تخريبية، مع إعطائه القدرة على ربط نفسه ببرامج أخرى ثم يتكاثر وينتشر داخل النظام المعلوماتي حتى يتسبب في تدميره تماما. وعرفه مركز الحسابات الشخصية القومي بالولايات المتحدة الأمريكية بأنه عبارة عن برامج مهاجمة تصيب أنظمة الحاسبات بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان، وهي في العادة برنامج صغير مكتوب بلغة معينة، ويقوم بالتجوال في الحاسب باحثا عن برنامج غير مصاب، وعندما يجد واحدًا ينتج نسخة من نفسه لتدخل فيه، وتتم هذه العملية في جزء من الثانية، حيث يقوم البرنامج فيما بعد بتنفيذ أوامر الفيروس.

د. عمر الفاروق الحسيني – المرجع السابق – ص 73، د. هدى قشقوش – جرائم الكومبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي في الفترة من 28,25 أكتوبر 1993 – ص 13.

المطلب الأول - المقصود بإتلاف البرامج والمعلومات:

الإتلاف أو التخريب هو التأثير على مادة الشيء، بحيث يذهب أو تقل قيمته الاقتصادية، والإتلاف لا يشترط فيه إفناء مادة الشيء ولكن يتحقق ذلك بكل فعل من شأنه أن يجعل الشيء غير صالح للاستخدام المعد له.

والإتلاف لغة: إذهاب الشيء، يقـال: تلف الشيء، أي؛ هلك[1] ويقرب من هذا المعنى الاصطلاحي للإتلاف: فهو إخراج الشيء من أن يكون منتفعاً به منفعة مطلوبة منه عادة[2].

وهناك صور لإتلاف البرامج والمعلومات، هي:

1- محو البيانات إلكترونياً بتدميرها أو جزء منها.
2- إدخال بيانات في نظام المعالجة الآلية لم تكن موجودة مما يؤدي إلى التشويش على صحة البيانات القائمة.
3- تعديل البيانات أو تعديل طرق انتقالها، أو تعديل وسائل هذا الانتقال[3].

1- انظر: القاموس المحيط، فصل التاء، مادة (تلف).

2- انظر: بدائع الصنائع 164/7.

3- انظر: الحماية الجنائية للبيانات المعالجة إلكترونياً، د/ علي بن عبد القادر القهوجي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، عام2000م. دراسة تجارب الدول في مجال أحكام في المعلوماتية، إعداد: د/ محمد القاسم، د/ رشيد الزهراني عبد الرحمن السند، عاطف العمري، مشروع الخطة الوطنية لتقنية المعلومات 1423/11/10هـ. العقود الإلكترونية، عبد الوهاب بدري – مجلة عصر الحاسب، تصدر عن جمعية الحاسبات السعودية – العدد الخامس، عام 2001م، ص52. انظر: النظام القانوني لحماية التجارة الإلكترونية، د/ عبد الفتاح بيومي حجازي، دار الفكر الجامعي الإسكندرية، الطبعة الأولى عام، 2002م، 118/1. النظام القانوني لحماية التجارة الإلكترونية، د/ عبد الفتاح بيومي حجازي، دار الفكر الجامعي الإسكندرية، الطبعة الأولى، عام 2002م، 118/1.

إن من الجرائم المتعلقة بالحاسب الآلي جريمة إتلاف برامج ومعلومات الحاسب الآلي، وهذه الجريمة تعد من جرائم الاعتداء، حيث تتمثل في إتلاف البرامج أو المعلومات المرتبطة بالحاسب الآلي.

المطلب الثاني - إتلاف البرامج والمعلومات ببرامج فيروسية:

فيروس الحاسب الآلي عبارة عن برنامج يتم تسجيله أو زرعه على الأقراص أو الأسطوانات الخاصة بالحاسب الآلي، ويظل خاملاً لفترة محددة، ثم ينشط فجأة في توقيت معين ليدمر البرنامج أو المعلومات المخزنة أو يتلفها جزئياً وذلك بالخرق أو التعديل، ومن هنا يعتبر الفيروس شديد الصلة بالجريمة، فهو أداة لارتكابها حيث يؤدي إلى تعطيل أو إفساد نظام المعالجة الآلية، أو إلى محو وتعديل البيانات. إن أبرز خصائص فيروس الحاسب الآلي القدرة على النسخ الذاتي التلقائي، فهو عبارة عن برنامج أو مجموعة تعليمات وأوامر للحاسب الآلي تلحق الضرر بنظام المعلومات أو البيانات، وتكون له القدرة على التضاعف والانتشار بأن يقوم عند تشغيله بزرع نسخ منه في الأقراص الصلبة[1]، فهو ينسخ نفسه عدة مرات وينتشر عبر خطوط التوصيلات الإلكترونية، ويصدر معلومات غير صحيحة ويؤدي في النهاية إلى تدمير النظام، وإتلاف البيانات والمعلومات.

1- انظر: الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني، د.هدى حامد قشقوش، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، عام 2000م ص13. الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، د/ هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، 2000م، ص48،49. التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت، عماد علي الخليل، عمان الأردن، عام2000م، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، ص4. التكنولوجيا الحديثة والاتصال الدولي والإنترنت، د/ علي محمد شمر، الشركة السعودية للأبحاث والنشر، جدة، المملكة العربية السعودية، 1997م، ص244.

خصائص الفيروسات المعلوماتية:

تتمثل خصائص الفيروسات المعلوماتية وفقا للتعريفات المتقدمة بالقدرة على الاختراق، والاختراق في القانون العربي النموذجي، في شأن جرائم إساءة استخدام تقنية المعلومات بأنه "الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات، وذلك عن طريق اختراقه للإجراءات الأمنية"[1].

وجريمة الاختراق أو الدخول غير المشروع إلى نظم المعالجة الآلية للبيانات تشبه تماما الدخول إلى ذاكرة الإنسان، وهذا الدخول أو الاختراق له مدلول مادي يتمثل في أن الشخص قد يكون حاول الدخول، أو دخل بالفعل إلى النظام المعلوماتي، ووفقا للتصور المعنوي لفكرة الدخول، فإنه يتحقق بأيِّ صورة من صور التعدي، أي؛ يستوي أن يكون التعدي مباشرا أو غير مباشر، علما بأنّ الدخول في ذاته – حسب أنصار المدلول المعنوي – يعد جريمة وقتية، وإن تخلفت عنها بعض الآثار التي قد تستمر أو تأخذ برهة من الزمن[2]. ويتحقق الدخول بأيّ وسيلة تقنية وذلك عن طريق كلمة السر الحقيقة متى كان الجاني غير مخول في استخدامها أو باستخدام برنامج شفرة خاصة[3] أو عن طريق استخدام الرقم الكودي لشخص آخر أو الدخول برقم كودي شخصي لشخص مسموح له الدخول.

1- د. عبد الفتاح بيومي حمادي، مكافحة جرائم الكومبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، 2006، ص79.

2- د. أحمد حسام تمام – الجرائم الناشئة عن استخدام الحاسب الآلي – دراسة مقارنة – دار النهضة العربية 2000 ص 297.

3- د. مدحت رمضان – الحماية الجنائية للتجارة الإلكترونية – دار النهضة العربية – 2000 ص 51. د. هدى قشقوش – الحماية الجنائية للتجارة عبر الإنترنت – دار النهضة العربية 2000 ص36. دور البنية التحتية للمفاتيح العمومية في دعم الحكومة الإلكترونية في المملكة – د/ محمد بن إبراهيم السويل، ضمن البحوث المقدمة للقاء الحكومة الإلكترونية المعقود بمعهد الإدارة العامة بالرياض، يوم الثلاثاء 1422/11/15هـ. المخاطر الأمنية وطرق الحماية منها – تركي بن أحمد العصيمي – دار المعارج – الرياض – الطبعة الأولى – عام 1420هـ، ص39. التوقيع الإلكتروني، د/ أحمد شرف الدين، مؤتمر التجارة الإلكترونية والإفلاس عبر الحدود القاهرة، عام 2000م، ص1.

الشفرة حسب القانون السالف ذكره هو مفتاح أو مفاتيح سرية خاصة لشخص أو لجهة معينة تستخدم لتزويد البيانات الحاسوبية بالأرقام. والتشفير في حد ذاته إجراء يؤدي إلى توفير الثقة في المعاملات الإلكترونية وذلك باستخدام أدوات أو وسائل أو أساليب لتحويل المعلومات، بهدف إخفاء محتوياتها والحيلولة دون تعديلها أو استخدامها بطريقة غير مشروعة[1]. ونظام التشفير يتلافى بعض المخاطر المتوقعة من استخدام الطرق الإلكترونية في المعاملات التجارية، وهناك طريقتين أكثر استخداما أولهما التشفير السيمتري Symetringue ثم تطور الأمر إلى نظام Asymétrique وهو وسيلة تتيح استخدام العديد من الأرقام التي يتعذر تزويرها[2]. وهناك الطريقة الثانية في التشفير، هي بطريقة المفتاح العام وهي سلسلة من الهندسة العكسية Algorithm تستخدم مفتاحين مختلفين أحدهما للتشفير والآخر لفك الشفرة، والمفتاح العام يمكن معرفته لبعض الجهات المختصة ولا يقصد منه أن يبقى سرا.

وسنعرض للقدرة على الاختفاء، وللقدرة على الانتشار، وللقدرة على التدمير المعلوماتي.

القدرة على الاختراق:

تزود البرامج الفيروسية بما يمكنها من اختراق النظم المعلوماتية والمواقع الإلكترونية المحاطة بنظم أمنية، وأشهر مثال لذلك فيروس حصان طروادة الذي يتم من خلاله استخدام الحيل والخدع كي يتمكن من دخول النظام المعلوماتي وتدميره أو إفساده وتعطيله عن العمل وذلك من خلال الارتباط ببرامج مفيدة للمستخدم يتم تحميل الفيرس المعلوماتي معها.

1- د. مدحت رمضان – مرجع سابق صـــ 31، د. عبد الفتاح حجازي – مرجع سابق ص48.

2- د. هدى حامد قشقوش – الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت – دار النهضة العربية – القاهرة – 2001 – ص76.

القدرة على الاختفاء:

يتم تزويد الفيرس المعلوماتي بما يمكنه من التخفي والتمويه حتى لا يتم اكتشافه من قبل المواقع المستهدفة، فهناك فيروسات تدخل للنظام المعلوماتي في صورة ملفات متخفية، وأبرز مثال على ذلك الفيروسات المنطقية والزمنية.

القدرة على الانتشار:

إن سرعة الانتقال من نهاية طرفية إلى باقي الأطراف الداخلة في الشبكة في ثوانٍ معدودة بسبب التكاثر اللانهائيِّ، وقد ساعد على هذا الانتشار التوافق فى البرامج المستخدمة على نطاق واسع عبر دول العالم، وشبكات المعلومات (الإنترنت)[1].

القدرة على التدمير:

الهدف الأساسي للفيروس المعلوماتي هو تدمير وتخريب المعلومات والبرامج بما يؤدي في النهاية إلى تعطيل أو توقف النظم المعلوماتية، فإن الفيروس يتجه إلى مكان ما في الذاكرة ويظل كامنا[2]، حتى يتحقق الأمر أو الزمن الذي يعتمد برمجة المفجر في الفيروس عليها، ثم ما يلبث أن يقوم بنشاطه في تدمير المعلومات[3].

1- Arabian Computer News, Vol.61. Mar. 1989. PP. 10-11.

2- انظر: الإنترنت والقانون الدولي الخاص: فراق أم تلاق؟، للدكتور / أحمد عبد الكريم سلامة، ضمن أبحاث مؤتمر (القانون والكمبيوتر والإنترنت) المجلد الثاني، ص28. التجارة الإلكترونية، تأليف / روب سميس، ومارك سبيكر، ومارك تومسون – ترجمة: د/ خالد العامري، دار الفاروق للنشر والتوزيع، القاهرة – مصر، عام 2000م، ص 98. التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الإثبات المدني، دراسة مقارنة، للدكتور/ عباس العبودي، مكتبة دار الثقافة والنشر والتوزيع، عمان، الأردن ص40. د. عمر الفاروق الحسيني – المرجع السابق – ص73، د. هدى قشقوش – جرائم الكومبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي في الفترة 25–28 أكتوبر 1993 ص 13. الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، د/ هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، 2000م، ص48،49.

3- David Febrache: Pathology of computer viruses , Springs Overlay, New York, 1992.P.30

صور من الإتلاف المعلوماتي:

للإتلاف المعلوماتي صور وأشكال متعددة، فمنها ما يؤثر على ماديات النظام المعلوماتي بتعطيلها وإيقافها عن العمل- ويخرج من نطاق البحث تلك الحالة التي يكون فيها الإتلاف بالطرق المادية بالكسر والتخريب إلى غير ذلك من الطرق- ونقصر البحث على استخدام الطرق التقنية في الإتلاف المعلوماتي:[1]

1- الاعتداء على المعلومات مما يؤدي إلى إعاقة وتعطيل النظام عن العمل:

وينجم عن فعل يتسبب في تباطؤ أو ارتباك عمل نظام المعالجة الآلية للمعلومات، ويترتب على ذلك تغير في حالة عمل النظام. ويسوّي بعضهم بين عرقلة النظام عن العمل ومحو أو تعديل أو إلغاء المعلومات، وحتى يمكن أن تتحقق الفاعلية في الإتلاف ينبغي أن يوجه لبرامج تشغيل النظام المعلوماتي وليس على المعلومات بالمعنى الضيق، سواء أكان نظام التشغيل يتعامل مع معلومات مالية تجارية واقتصادية أم شخصية[2].

2- العدوان على المعلومات المخزنة بالنظام المعلوماتي:

تقع صورة الإتلاف المعلوماتي بتدمير وإتلاف وتخريب المعلومات المخزنة بالنظام المعلوماتي ويتحقق ذلك بتدمير وإتلاف وتخريب المعلومات المخزنة بالنظام المعلوماتي بحيث تصبح بلا معنى ولا يمكن الاستفادة منها، وهو لا يسري على النظام المعلوماتي ككل، وعلى التعاملات الإلكترونية[3].

1- د. محمد زكي عبد المجيد وآخرون – فيروسات الحاسب وأمن البيانات – موسوعة دلتا كومبيوتر مطابع المكتب المصري الحديث 1992 ص36، د. ماجد عمار – المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكومبيوتر ووسائل حمايتها – دار النهضة العربية – 1989 ص35، د. حسيني منصور – المرجع السابق – ص 292-293.

2- انظر: الحماية الجنائية للتجارة الإلكترونية للدكتور/ مدحت عبد الحليم رمضان، ص131، دار النهضة العربية – القاهرة. الصحوة الإسلامية – ضوابط وتوجيهات – للشيخ محمد بن صالح بن عثيمين ص178، دار القاسم – الطبعة الثالثة – 1416هـ. الإنترنت والتجارة الإلكترونية – صلاح حامد رمضان على – نشرة تصدر عن شركة الراجحي المصرفية للاستثمار ص34، العدد: 12 / ذو الحجة / 1421هـ. د. أحمد حسام تمام – المرجع السابق – ص352.

3- د. عبد الفتاح بيومي حجازي – المرجع السابق – ص40، د. نائلة قورة – المرجع السابق – ص196، د. عزة محمود أحمد خليل – المرجع السابق – ص37، د. عبد الحق حميش – حماية المستهلك

3- تضخيم البريد الإلكتروني:

أن يتم إرسال نسخ مكررة بعدد كبير من الرسائل، بما يترتب عليه إعاقة سير النظام التقني المعلوماتي بشكل من ضبط، ويؤدي ذلك الأمر إلى إعاقة استخدام تلك الخدمة أو توقفها وفي الغالب يتم هذا الأمر من خلال فيروسات معلوماتية يتم بثها ونشرها عن طريق الإنترنت[1].

بث الفيروسات المعلوماتية عبر شبكة المعلومات لتعطيل الاتصالات:

وتعد جريمة بث الفيروسات من أخطر التهديدات التي تضر شبكة المعلومات، فمنها الجريمة التي لا تقع ضد المعلومات أو البرامج بل تتم ضد تعطيل أو إيقاف شبكة الاتصالات من خلال تدمير أو إتلاف وتخريب برامج الاتصال[2]، وتتحقق صورة الإتلاف المعلوماتي تلك من خلال القيام بإدخال أو تعديل أو محو المعلومات أو البرامج[3].

الإلكتروني – بحث مقدم إلى مؤتمر الأعمال المصرفية بين الشريعة والقانون – كلية الشريعة والقانون وغرفة تجارة وصناعة دبي – الإمارات العربية المتحدة – 10-12 مايو 2003 ص1267.

Fishnigni Deborah: National and international Aspects of computer crime , the emerging need for statutory controls , theses of , London , center for criminal law studies , Westfield , 1993.p.209

1- د. عمر محمد يونس – الجرائم الناشئة عن استخدام الإنترنت – دار النهضة العربية 2004 ص351.

2- د. عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية – 1988 – ص 48. نظام حماية حقوق المؤلف في المملكة العربية السعودية، إعداد: عبيد الله محمد العبيد الله، ضمن دورة حقوق الملكية الفكرية (الأنظمة والتشريعات) المعقودة بتاريخ 1422/11/12هـ في مركز الملك فيصل للبحوث والدراسات الإسلامية – معهد الفيصل لتنمية الموارد البشرية. د. جميل عبد الباقي – الإنترنت والقانون الجنائي – المرجع السابق – ص63.

3- انظر: الفقه الإسلامي وأدلته، للدكتور/ وهبة الزحيلي، دار الفكر، دمشق – 1417هـ، 8/4، الحق ومدى سلطان الدولة في تقييده، للدكتور/ فتحي الدريني، جامعة دمشق – 1386هـ، ص 184. د. عبد الفتاح بيومي حجازي – المرجع السابق – ص 46.

نخلص من ذلك أن التطور الهائل في نظم الاتصالات عن طريق شبكة المعلومات العالمية الإنترنت أدى إلى سرعة انتقال الفيروس، وإلى إصابة العديد من أجهزة وبرامج المتعاملين بالحاسب الآلي به.

من أبرز الوسائل التي تساعد على انتشار الفيروس:

1- البريد الإلكتروني (E-mail)، فيتم إرسال الفيروس عبر البريد الإلكتروني لعدد ضخم من المتعاملين بالإنترنت، فعند فتح الرسالة يصيب الفيروس نظام المعالجة الآلية، ويدمر البيانات والمعلومات المخزنة فيه.
2- نسخ البرامج، يتم انتقال الفيروس إلى البرنامج أو المعلومات داخل جهاز الحاسب الآلي عن طريق إدخال برنامج منسوخ مصاب بالفيروس إلى الجهاز فتنتقل العدوى إلى البرامج والمعلومات.
3- تحميل برامج من الشبكات، قد يؤدي تحميل برامج من الشبكات إلى الإصابة بالفيروس، وإتلاف البرامج والمعلومات المخزنة داخل الحاسب الآلي، ومن هذه البرامج: برامج ضغط البيانات، فإن كثيراً من المتعاملين يستخدم هذه البرامج في ضغط البيانات (Compression) من أجل توفير مساحات تخزينية، فربما كانت هذه البرامج محملة بالفيروس(1).

إن من خصائص الفيروس قدرته على الاختفاء والتمويه على المستخدم حيث إنه يرتبط ببعض البرامج التي تؤدي أعمالاً نافعة ثم يدخل إلى النظام عند تشغيل هذه البرامج، ويقوم بنسخ نفسه في كل مكان يستطيع الوصول إليه.

ومن أمثلة الفيروسات التي أحدثت آثاراً مدمرة: فيروس أصاب ملايين الكمبيوترات في العالم خلال شهر أكتوبر 2002م، يحمل اسم (بغبير) الذي ينتقل بسرعة هائلة عبر البريد الإلكتروني، وهو ينتمي إلى تلك الفيروسات التي يسميها المتخصصون في أمن المعلومات بالدودة متعددة الأخطار لأنه يهاجم كلمة السر وأرقام بطاقات الاعتماد، والبريد

1- انظر: جرائم الكمبيوتر والإنترنت، محمد أمين الرومي، ص59.

الإلكتروني، ويتكاثر بسرعة كبيرة ويمتلك قدرة كبيرة على تعطيل البرامج المضادة للفيروسات، ولذلك يعتبر من أعنف الفيروسات التي أطلقت حتى الآن، وفيروس بغبير يصل على شكل ملف مرفق برسالة إلكترونية، ويحمل أسماء أصدقاء أو زملاء في العمل، ويدخل إلى صفحات وعناوين مستخدمي الإنترنت لينتقل بسرعة كبيرة في رسائل جديدة[1].

المبحث الثاني
محل جرائم الإتلاف المادي والإتلاف المعلوماتي

تناول المشرع الجنائي المصري جرائم الإتلاف في باب الإتلاف والحريق وقد خصص لها المشرع قسمًا في الباب الثالث عشر تحت عنوان التخريب والتعييب والإتلاف بالمواد 354–368 ق.ع.م وقد تعددت نصوص تجريم الإتلاف وما في حكمه بقانون العقوبات المصري، تنص المادة 361ق.ع.م على أن "يعاقب كل من خرب أو أتلف عمدا أموالا ثابتة أو منقولة لا يمتلكها أو جعلها غير صالحة أو عطلها بأية طريقة"[2]. وتقابل المادة 361 ق.ع.م المادة 434 من قانون العقوبات الفرنسي القديم، والتي تنص على عقاب كل من خرب أو أتلف أموالا ثابتة أو منقولة مملوكة للغير وتناول أركان تلك الجريمة من حيث المحل والركن المادي والركن المعنوي.

1- محل الجريمة المعلوماتية:

يعتبر بعضهم أن نص المادة 361 ق.ع.م هو نص عام بالنسبة لجرائم الإتلاف ويقوم بدون النص الاحتياطي بالنسبة لجرائم الإتلاف فما لم يدخل في نطاق النصوص الخاصة سيدخل حتما ضمن نطاق هذه المادة نظرا لأن محلها يشمل جميع أنواع الأموال المادية الثابتة أو المنقولة فيقع الإتلاف على كل مال ثابت أو منقول إلا ما خرج عن حكمه بنص خاص. ولا تثير مسألة إتلاف البيانات المسجلة على دعامة مادية (ديسك،

1- انظر: جريدة الرياض، العدد: 12521، السبت 28 / رجب / 1423هـ، ص1 من ملحق الجريدة.

2- د. عمر الفاروق الحسيني – المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية – ط2، 1992، ص69.

أسطوانة.... إلخ) صعوبة قانونية لأن الدعامة تعد مالا منقولا يحميه التجريم في جرائم الأموال، وإنما تثار الصعوبة في حالة كون المال الذي يقع عليه الإتلاف في صورة معلومات لأن المال هنا ذو طبيعة معنوية[1].

يتفق الفقه على أنه فيما يتعلق بالاعتداء بالإتلاف والتخريب على الجانب المادي من نظم المعلومات فإنه يتوافر فيها وصف المال المنقول، وبالتالي يخضع الاعتداء عليها لجريمة الإتلاف وذلك كمن يقوم بكسر وتحطيم جهاز الحاسب الآلي، بل والبرامج والمعلومات متى كانت مسجلة على دعامة مادية[2].

وذهب الاتجاه المؤيد لتطبيق النصوص التقليدية:

نص المادة 361 ق.ع.م جاء عاما بالنسبة للأموال محل الجريمة ولم يرد فيه ما يدل على قصدها على المنقول المادي فقط، بما يعني إمكانية تطبيقها على الأموال المنقولة سواء أكانت مادية أم معنوية. عدم تحديد المشرع لوسيلة معينة يقع بها الإتلاف باعتبارها من الجرائم ذات القالب الحر، الاعتراف للبرامج والمعلومات بوصف المال واعتبارها تقف

1- د. حسن صادق المرصفاوي – المرصفاوي في قانون العقوبات – منشأة المعارف بالإسكندرية سنة 2001 ص323، د. محمد سامي الشوا – الجرائم المعلوماتية للتعدي على الذمة المالية للغير، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون – كلية الشريعة والقانون وغرفة التجارة والصناعة، دبي – الإمارات العربية المتحدة 10-12 مايو 2003 ص 1079، د. غنام محمد غنام – عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر ص12.

2- د. جميل عبد الباقي – المرجع السابق – ص 154، د. غنام محمد غنام – عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر – بحث مقدم لؤتمر القانون والكومبيوتر والإنترنت خلال الفترة من 1-3 مايو 2000 ص 21، د. حسام تمام – المرجع السابق – ص347، د. محمود محمود مصطفى– شرح قانون العقوبات – القسم الخاص – طـ8 – 1984 ص647 فقرة 550.

Deveze (J.): Commentaire de la loi No. 88 – 19 du 5 Jan. 1988, relative a la Froude informatique, la droit de l'informatique 1987, mise a jour Février, 1988, No. 26

على قدم المساواة مع المال المادي. إن في عدم الاعتراف للكيان المعلوماتي بالحماية سيكون فيه رفض لتطوير المفاهيم القانونية وتجريد لها من الحماية الجنائية[1].

الركن المادي في الجريمة المعلوماتية:

النشاط الإجرامي هو الإتلاف، ويعرّفه الفقه بأنه "كل فعل من شأنه أن يؤثر في مادة الشيء أو في قيامه بوظائفه المختلفة على نحو يذهب من قيمته على النحو غير المعتاد لقيمة الشيء مع مرور الزمن مع قصد الإضرار بالغير"[2]. ويعد قيمة الشيء هو محل الحماية الحقيقي وليست مادته، حيث إنّ مادته هي الوسيلة لحماية قيمته[3].

ويقصد بالتخريب توقف الشيء تماما عن أن يؤدي منفعة حتى وإن لم تغنى مادته سواء أكان هذا التوقف كليا أم جزئيا، ويرى بعضهم بأن التخريب والإتلاف مرادفان ويدلان على جعل الشيء غير صالح للاستعمال في الغرض المخصص له[4]. ويتجه جانب من الفقه بأن هناك فرقا يتمثل فى أن الإتلاف يكون جزئيا للشيء، بمعنى أنه يمكن إصلاحه إلا أن صلاحيته للاستعمال انقضت، أما في التخريب يعني أن الشيء لم يعد قابل للإصلاح[5].

1- د. علي عبد القادر القهوجي – المرجع السابق – ص78، د. هدى قشقوش – جرائم الحاسب الإلكتروني – دار النهضة العربية 1992 ص 44، د. عزة محمود خليل – فيروسات الحاسب – مرجع سابق ص258، د. محمد حسام لطفي – جرائم الكومبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي في الفترة من 25-1993/10/28 ص 61.

2- د. محمود نجيب حسني – القسم العام – مرجع سابق – ص 88 فقرة 979

3- د. أحمد فتحي سرور– الوسيط في قانون العقوبات – القسم الخاص – ط4 – دار النهضة العربية – 1991 – ص 303.

4- د. رمسيس بنهام – الجرائم المضرة بالمصلحة العمومية – الإسكندرية – منشأة المعارف 1985 – ص 244.

5- د. محمود نجيب حسني – جرائم الاعتداء على الأموال في قانون العقوبات اللبناني – دراسة مقارنة 1984 ص496 فقرة 532.

ويقصد بعدم الصلاحية للاستعمال جعل الشيء لا يقوم بوظيفته المرصود لها على النحو الأكمل. والتعطيل هو توقف الشيء عن القيام بوظيفته فترة مؤقتة ويكفي أيا من هذه الأفعال حتى تقع الجريمة، فالاختلاف بين الإتلاف والتعييب اختلاف كميٌّ يتعلق بمدى ما يترتب على الفعل من ضرر بالنسبة لمادة الشيء وقيمته، علما بأنه ليس بشرط في الركن المعنوي، فلا يشترط في الإتلاف أن يكون تاما، بل يمكن أن يكون جزئيا، ولكن يشترط في حالة الإتلاف الجزئي أن يكون من شأنه جعل الشيء غير صالح للاستعمال أو تعطيله(1).

ويلاحظ على هذا النص القانوني عدم تقييد المشرع النشاط الإجرامي بوسيلة، مما يعني أن هذه الجريمة تدخل ضمن نطاق الجرائم ذات القالب الحر، كما أنّ النص اتسم بتعدد النتائج التي جرمها المشرع وهي الإتلاف أو التخريب أو التعييب أو التعطيل(2)، ويلاحظ أيضا أن المشرع لم يجرم نتيجة واحدة بل جرم نتائج متعددة وهي الإتلاف والتخريب وعدم الصلاحية للعمل والتعطيل(3). ولا يعد إتلافا أو تعييبا استعمال الشيء دون رضاء مالكه، ولكن على الوجه المعد له، ما لم يكن استعمالا مفرطا من قيمته، أما استعمال الشيء في غير الوجه المعد له، فيعد عيبا، إذا أفضى ذلك إلى الانتقاص من قيمته.

الركن المعنوي:

جريمة الإتلاف أو التخريب من الجرائم العمدية، ويتخذ ركنها المعنوي صورة القصد الجنائي بعنصري العلم والإرادة، فليزم أن يعلم الجاني أن المال الذي يقع عليه فعله مملوك للغير، وأن من شأنه فعله التأثير في مادة الشيء أو في قيمته، أو كفاءته.

لتحقيق المطلوب منه، وبتوافر عنصر الإرادة باتجاه إرادة الجاني إلى الفعل الإجرامي بتخريب أو إتلاف أو إعدام الصلاحية أو التعطيل للمال المملوك، فإذا وقع الفعل بطريقة خاطئة، فإنه يخضع لنص آخر هو نص المادة 378 – 6 ق ع م التي تعاقب من

1- د. جميل عبد الباقي الصغير – القانون الجنائي والتكنولوجيا الحديثة – الكتاب الأول – جرائم الأموال الناشئة عن استخدام الحاسب الآلي – دار النهضة العربية 1992- ص ـــ154.

2- د. عبد القادر القهوجي – المرجع السابق – ص78.

3- د. محمود نجيب حسني – المرجع السابق – ص498 فقرة 533.

يتسبب في إهماله بإتلاف منقولات مملوكة للغير بالغرامة[1]، ولم يشترط المشرع توافر قصد خاص في قيام تلك الجريمة ويكتفي في قيامها بتوافر القصد العام[2].

المطلب الأول - تطبيقات جرائم الإتلاف المعلوماتي:

وقد صدر في القانون الجنائي المصري بعض النصوص الجنائية التي تحمي جوانب من الاعتداءات المعلوماتية ونرى مدى قدرتها على الحماية من الإتلاف المعلوماتي حيث:

1. تجريم المشرع المصري للاعتداء على حاسبات وشبكة معلومات مصلحة الأحوال المدنية.
2. تجريم مشروع قانون التجارة الإلكترونية المصري للإتلاف المعلوماتي.
3. تجريم قانون التوقيع الإلكتروني رقم 15 لسنة 2004 والإتلاف المعلوماتي.

وسنعرض لموقف المشرع من القوانين المختلفة لحماية المجتمع من جريمة الإتلاف المعلوماتي وبخاصة من حيث كفايتها.

أولا – تجريم المشرع المصري الاعتداء على حاسبات وشبكة معلومات مصلحة الأحوال المدنية:

جرم المشرع المصري الاعتداء على حاسبات وشبكة معلومات مصلحة الأحوال المدنية رقم 143 لسنة 1994 لحماية البيانات والمعلومات الخاصة بمصلحة الأحوال المدنية من الاعتداء على حاسباتها وشبكاتها.

وقد نص المشرع في هذا القانون بالمادة 74 على تجريم تلك الأفعال التي تقع على معلومات وبيانات خاصة بمصلحة الأحوال المدنية على أنه "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو غيره من القوانين يعاقب بالحبس مدة لا تتجاوز ستة أشهر، وبغرامة لا تزيد عن خمسمائة جنيه أو بإحدى هاتين العقوبتين – كل من أطلع

1- د. هشام فريد رستم – المرجع السابق – ص 321-322.

2- د. محمود محمود مصطفى – المرجع السابق – ص643 فقرة 552.

أو شرع في الاطلاع أو في الحصول على بيانات أو المعلومات التي تحتويها السجلات والحاسبات الآلية أو وسائط التخزين الملحقة بها أرقام بتغييره بالإضافة أو الحذف أو بإلغاء أو بالتدمير أو بالمساس بها بأيّ صورة من الصور أو أذاعها أو أفشاها في غير الأحوال التي نص عليها القانون ووفقا للإجراءات المنصوص عليها فيه، فإذا وقعت الجريمة على البيانات أو المعلومات أو الإحصاءات المجمعة تكون العقوبة السجن".

يؤكد بعضهم أن المشرع إدراكا منه لأهمية تلك المعلومات عمد إلى النص على حمايتها صراحة بنصوص خاصة، ومنها هذه المادة التي نص المشرع فيها على حماية المعلومات والبيانات المخزنة بحاسبات وشبكات مصلحة الأحوال المدنية من جميع صور الاعتداء بما فيها إتلاف المعلومات عندما ذكر الحذف أو الإلغاء أو بالتدمير أو المساس بها بأيّ صورة من الصور[1].

كما جرم المشرع المصري الاعتداء على شبكة المعلومات الناقلة لمعلومات مصلحة الأحوال المدنية فنصت المادة 57 من القانون على أن يعاقب.... كل من عطل أو أتلف الشبكة الناقلة لمعلومات الأحوال المدنية أو جزءًا منها، وكان ذلك ناشئا عن إهماله أو عدم مراعاته للقوانين واللوائح والأنظمة" ويشدد العقاب في حالة إذا وقع الفعل بطريقة العمد[2].

ويستفاد أن هذا التجريم قاصر على الاعتداء على الشبكة الناقلة لمصلحة الأحوال المدنية بتعطيلها أو إتلافها كليا أو جزئيا سواء أكان هذا الاعتداء عمدا أم بطريقة الخطأ[3].

1- د. أيمن عبد الحفيظ عبد الحميد سليمان – استراتيجية مكافحة جرائم استخدام الحاسب الآلي – مطبوعات جامعة المنصورة – سنة 2003 – ص 12.

2- الجريدة الرسمية ع 23 الصادرة في 9 يونيو 1994، د. عزة محمود خليل – المرجع السابق – ص173.

3- د. أيمن عبد الحفيظ – المرجع السابق ص19.

ثانيا – تجريم مشروع قانون التجارة الإلكترونية المصري للإتلاف المعلوماتي:

تضمن مشروع التجارة الإلكترونية المصري حماية مباشرة وغير مباشرة من أفعال الإتلاف المعلوماتي.

ا- الحماية المشددة من الإتلاف المعلوماتي:

نص مشروع القانون بالمادة 26 منه على أنه "مع عدم الإخلال بعقوبة أشد وردت في قانون آخر، يعاقب بالحبس وبغرامة مالية لا تقل عن 3000 جنيه أو بإحدى هاتين العقوبتين كل من دخل بطريقة الغش أو التدليس على نظام معلومات أو قاعدة بيانات تتعلق بالتوقيعات الإلكترونية، يعاقب بنفس العقوبة من اتصل أو أبقى الاتصال بنظام المعلومات أو قاعدة البيانات بصورة غير مشروعة[1].

1- محل الجريمة:

محل الجريمة هو التوقيع الإلكتروني، وقد عرفه مشروع القانون في فصل التعريفات ضمن تحديده للمصطلحات المستخدمه فيه، بأنه " حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتميزه عن غيره، "أي؛ أنه يعد مجموعة من البيانات أو المعلومات التي تسمح بتمييز معاملة الشخص صاحب التوقيع عن غيره وتلزم بالتصرف الذي قام به فهو بهذه المثابة يقوم بالدور ذاته الذي يقوم به التوقيع العادي" مع اختلاف المجال والشكل في مجال التوقيع الإلكتروني عن التوقيع العادي مع الاتحاد من حيث الوظيفة[2]. وتختلف قاعدة البيانات عن النظام المعلوماتي في أنها عبارة عن معلومات مخزنة يتم الرجوع إليها وقت الحاجة، أما النظام المعلوماتي فيتعلق ببرنامج تطبيقي لتشغيل الحاسب الآلي ويتفقان في أن كلاهما يتعلق بالتوقيع الإلكتروني[3].

1- د. أيمن عبد الله فكري – مرجع سابق – ص186.

2- د. حسن عبد الباسط جميعي – المرجع السابق – ص25. د. سعيد السيد قنديل – التوقيع الإلكتروني – دار الجامعة الجديدة للنشر – الإسكندرية 2004 – ص48.

3- د.عبد الفتاح بيومي حجازي – المرجع السابق – ص296-297.

الركن المادي للجريمة:

يتمثل الركن المادي في تلك الجريمة في الدخول بطريقة الغش أو التدليس لقاعدة البيانات أو النظام المعلوماتي الخاص بالتوقيع الإلكتروني، وكذلك عن طريق الاتصال أو الإبقاء على الاتصال غير المشروع الذي تم بطريقة الخطأ بقاعدة البيانات أو النظام المعلوماتي[1]، ولم يحدد المشرع المقصود بالدخول أو البقاء، ولكن يفهم من النص بطريقة اللزوم أنه الدخول أو بقاء في اتصال معلوماتي.

الركن المعنوي في الجريمة:

ووفقا للنص فإن هذه الجريمة من الجرائم العمدية يشترط فيها العلم بأن الجاني يقوم بانتهاك قاعدة بيانات أو نظام معلوماتي يتعلق بالتوقيع الإلكتروني، أو التسلل بالدخول إليه بأيّ وسيلة تدليسية أو بطريق الغش واتجاه إرادته للقيام بهذا النشاط الإجرامي، بل تقع الجريمة في حالة الاتصال بطريقة الخطأ بالنظام المعلوماتي الخاص بالتوقيع الإلكتروني، إذا أبقى الجاني على هذا الاتصال وتوافر قصد الغش، ينطبق على الإبقاء على الاتصال الذي تم بدون قصد نشاط الجاني هنا يقع بطريق[2] الامتناع عن قطع الاتصال الذي تم بطريق الخطأ، وتقدير توافر القصد الجنائي مسألة موضوعية يقدرها قاضي الموضوع على ضوء الوقائع الثابتة[3].

1- د. عمر الفاروق الحسيني – المرجع السابق – ص125.

2- وقد جرم المشرع الإنجليزي الولوج غير المسموح به لنظام الحاسب والصادر في 29 يونيو 1990 الذي بدأ تطبيقه في 29 أغسطس 1990، وقد احتوى هذا القانون على تجريم أفعال ثلاثة بموجب قانون إساءة استخدام الحاسب وهي: الدخول غير المصرح به على نظام الحاسب، الدخول غير المصرح به على نظام الحاسب لتسهيل ارتكاب فعل غير مشروع عن علم وتعمد، الدخول غير المصرح به على نظام الحاسب بواسطة زراعة برامج فيروس...

David Bain bridge: Ibid. P.249.

3- د. محمد حسام لطفي – المرجع السابق – ص 194.

ثانيا – الحماية الجنائية للإتلاف المعلوماتي:

تنص المادة 29 من مشروع قانون التجارة الإلكتروني المصري على معاقبة "كل من استخدم نظامًا أو برنامجًا للحيلولة دون إتمام المعاملات التجارية بالوسائل الإلكترونية، وذلك بالتعديل فيها أو محو بياناتها او إفسادها أو تدميرها أو بتعطيل أنظمتها". كما تنص المادة 31 على معاقبة كل من أدخل بعمد أو بإهمال فيروسًا إلى نظام معلوماتي بدون موافقة من مالك النظام أو حائزه الشرعي، وتنص المادة الأولى "على الحماية من الإتلاف المعلوماتي إذا كان من شأنه أن يترتب عليه التأثير على إتمام المعاملات التجارية بمنعها أو الحيلولة دون إتمامها"، وفي المادة الثانية تناول المشرع الوسيلة الأخطر في الإتلاف المعلوماتي وهي الفيروس ليجرم إدخالها للنظام المعلوماتي سواء أكان الفعل بطريقة العمد أم كان بطريق الخطأ.

كما جرم المشروع في قانون تنظيم التوقيع الإلكتروني المصري في المادة 12 منه أن الاعتداء على التوقيع الإلكتروني أو الوسيط الإلكتروني بالإتلاف أو التعييب أو التعديل أو التحوير أو بأي طريق آخر.

ثالثا – قانون التوقيع الإلكتروني رقم 15 لسنة 2004 والإتلاف المعلوماتي:

قرر المشرع المصري بهذا القانون تجريم العدوان على التوقيع الإلكتروني فجرم الاعتداء عليه بالإتلاف أو التعييب أو التخريب سواء على الكتابة الإلكترونية أو المحرر الإلكتروني أو التوقيع الإلكتروني إذا توافرت فيه الشروط التي نص عليها المشرع بالمادة 23 فقرة (ب) التي تنص على أن "يعاقب مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أيّ قانون آخر يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تتجاوز مائة ألف جنيه، أو زور شيئا من ذلك بطريقة الاصطناع أو التعديل أو التحوير أو بأيّ طريق آخر".

بل إنّ المشرع لم يقتصر في التجريم على الشخص الطبيعي بل اتجه إلى تجريم، ومعاقبة الشخص المعنوي في شخص المسؤول عن الإدارة الفعلية ما دام فعله هو الذي أدى

إلى ارتكاب الفعل المجرم ويعاقب على إهماله في هذا الشأن، فلا يشترط أن يتوافر لديه القصد الجنائي للمساهمة في ارتكاب الفعل بل يعاقب على الخطأ الناتج عن إهماله والذي يتسبب في ارتكاب الفعل المجرم.

وتعاقب المادة 24 من القانون المسؤول عن الإدارة، الفعلية للشخص الاعتباري المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة أسهم في وقوع الجريمة مع علم بذلك[1].

فالمشرع لا يعتد بالوسيلة المستخدمة في ارتكاب الجريمة[2]، بنص المادة 23 فقرة (هـ) من القانون بتجريمها للحصول بأيّ وسيلة وبدون وجه حق على توقيع أو وسيط أو محرر إلكتروني أو اختراق هذا الوسيط أو اعتراض أو عطله عن أداء وظيفته[3].

المطلب الثاني - الإتلاف في القانون الجنائي الفرنسي:

مر التطور التشريعي في مواجهة الإتلاف المعلوماتي في القانون الفرنسي بمرحتلين: ففي البداية كان التجريم من خلال تطبيق النصوص الجنائية التقليدية في جرائم الإتلاف في القانون رقم 288/19 ثم بنصوص خاصة في نص المادة 2/246، وفي المادة 462 -463.

التجريم في نطاق النصوص التقليدية:

لم يختلف المشرع في القانون الفرنسي بالنسبة للحماية الجنائية للمعلوماتية في نطاق النصوص العامة والمتعلقة بإتلاف الأموال بالمواد من 434- 439[1]. ولقد انقسم الفقه الفرنسي في محاولته تطبيق هذه النصوص التقليدية على الإتلاف المعلوماتي إلى اتجاهين:

1- منشور بالجريدة الرسمية ع (23) الصادر في 9 يونيو 1994 (S.(www.isdo.gov.eg

2- واللائحة التنفيذية للقانون بجريدة الوقائع المصرية العدد 115 في 25 مايو 2005

3- كما نصت على ذلك المادة 31 من المشرع قانون التجارة الإلكتروني المصري، راجع د. هدى قشقوش – الحماية الجنائية للتجارة الإلكترونية – المرجع السابق – ص101.

الاتجاه الأول:

ويرى أن النصوص التقليدية لا تسمح بتطبيقها على جرائم المعلوماتية، ويستند أنصار هذا الاتجاه إلى الأسانيد الآتية:

1. انتفاء الصفة المادية للنبضات الكهربائية التي تختزن البرامج والمعلومات.
2. البرامج والمعلومات لا تعتبر مالا وفقا للتصور التقليدي للمال.
3. إنّ التأثير في وظائف نظم المعلومات عن طريق الإضرار بالمعلومات لا يعد إتلافا وفقا للمفهوم التقليدي، وإنّ التوسع في التأويل يخالف مبدأ الشريعة الجنائية[2].

ونخلص من ذلك إلى أن نصوص الإتلاف التقليدية لا تحمي سوى المال المتمثل في ثروة محسوسة، والذي يكون محلا للملكية التقليدية في مواجهة الاعتداءات المادية[3].

الاتجاه الثانى:

رأى العديد من الفقهاء الفرنسيين أن نصوص الإتلاف الموجودة بالقانون الجنائي الفرنسي على الإتلاف المعلوماتي وذلك استنادا إلى الحجج والمبررات التالية: لم يشترط المشرع الفرنسي أن يكون الإتلاف قاصرا على أن يكون المال ذو طبيعة مادية وإنما تشمل تلك القيم المعلوماتية الحديثة[4]. إذا وقع الإتلاف المعلوماتي على الكيان المعلوماتي، فإنه بالتبعية يحدث ضررا بالمال بوسيلة معينة، أيا كانت هذه الوسيلة[5].

1- S.(www.legifrance.gouv.fr).

2- Masse: le droit pénal ne de l'informatique en informatique et droit pénal.p32 , Pradel et feuillard: les infraction commise au moyen de l'ordinateur,R.Dr.pen.et crime 1985.p.307 , Barit (M.): le fraudé informatique , une approche de droit comparé,Rev.D.P.C,No.4 avril, 1985, p.296, Amdre Lucas: le droit de l'informatique, P.U.F 1993.P. 519

3- Devez (J.): la fraudé informatique, aspects Juridiques, J.C.P 1987 – 1-3289

وتطبيقا لذلك فقد صدر حكم محكمة استئناف Anvers برفض تطبيق المادة 434 ق ع ف القديم على خبير نظم المعلومات نسب إليه مباشرة لأفعال تفريغ ترتب عليها إعاقة مادية للنظام، راجع د. أيمن فكري – المرجع السابق – ص 197.

4- Tiedeman: fraude et autres délits d'affaires commis 'a l'aide d'ordinateurs électroniques R.D.P.C 1984.P.618

5- Lucas Andrée: op.cit.p.521

وبالرجوع إلى التطبيقات القضائية نجد أنّ الأحكام القضائية أخذت بالاتجاه الأول، ولذا فقد تدخل المشرع الجنائي الفرنسي، لكي يضع النصوص الجنائية الخاصة بالإتلاف المعلوماتي في القوانين المتعاقبة بداية من قانون 6 يناير 1978 الذي يعد من أوائل القوانين الفرنسية التي أراد بها المشرع الفرنسي مواجهة الإجرام المعلوماتي[1]. ثم صدرت مجموعة قوانين أهمها القانون الصادر في 3 يوليو 1985 الخاص بحماية البرامج في ضوء الملكية الفكرية ثم القانون رقم 88/19 الذي أراد به المشرع الفرنسي حماية أنظمة المعلومات نظرا لكثرة استخدام الفيروسات التي عرفت تحت مسمى الإرهاب المعلوماتي.

الحماية الجنائية للإتلاف المعلوماتي في القانون رقم 88/19:

1. دخول بطريقة الغش في النظام المعلوماتي:

اشتمل القانون رقم 88/19 على تجريم مجرد الدخول غير المصرح به للنظام المعلوماتي، ويمكن أن نطلق عليه الحماية غير المباشرة، والحماية من الإتلاف المعلوماتي بطريقة غير مباشرة وردت في القانون رقم 88/19 وردت بالمادة 462–2 التي تنص على معاقبة كل من يقوم بشكل احتيالي بالدخول أو الاحتفاظ بكل أو بجزء من أيّ نظام للتشغيل الآلي الخاص بالمعطيات، وهي الجرائم الشكلية لهذا النشاط الإجرامي الذي يعاقب عليه بشكل منفرد، دون أن يتطلب القانون توافر نتيجة معينة، ذلك أن مجرد الدخول أو الاحتفاظ بالمعلومات، وعلى هذا فهذا يقوم النص على حماية النظام الذي يحتوي على المعلومات قبل أن تنظر في حماية المعلومات ذاتها، وتلك طريقة لحماية المعلومات التي لم يقدر النص على وضع حماية لها.

كما أن هناك تلازمًا بين الإتلاف المعلوماتي وجريمة الولوج أو البقاء بطريقة غير مشروعة في النظام المعلوماتي، ويتكون النشاط الإجرامي في هذه الفقرة من المادة 462 من فعلين:

1- Michel Kreisler: l'investissement informatique de l'entreprise et sa protection pénal, G.P. 1990,P.6

1- الدخول بطريقة الغش في اتصال مع نظام المعالجة الآلية للمعلومات.
2- الإبقاء على الاتصال وعدم الخروج منه حالة كونه تم بطريقة الخطأ، ويتكون النشاط الإجرامي في جريمة الولوج غير المشروع كغيره من الجرائم من الركن المادي والركن المعنوي.

أولا - الركن المادي:

هو نشاط إيجابي من جانب الجاني يتمثل في الدخول في الاتصال بطريقة الغش مع نظام للمعالجة الآلية للمعلومات كله أو في جزء منه، ومفهوم الدخول في نص القانون لا يقصد به الدخول المادي بل الدخول المعنوي، أي؛ الاتصال بالنظام محل الحماية بالطرق الفنية المعلومة[1].

للدخول على المواقع الإلكترونية[2]، وكما في حالة من يقوم بإقامة وصلة لربط خط تلفوني مع خط آخر للاتصالات عن بعد لإرسال واستقبال المعلومات، أو من يقوم بإنشاء تحويلة أو من يلتقط من مسافة الإشعاعات التي تصدر عن النظم المعلوماتية[3]، وهو يعرف بالتداخل أو الالتقاط المعلوماتي[4]، وأن يتم الدخول ضمن مفهوم الولوج أو الدخول المعلوماتي كل من يستطيع الوصول للنظام المعلوماتي بطريقة مباشرة أو غير مباشرة[5].

ويتبين لنا من النص أنه يتسع ليشمل كل شخص لا يحق له الاتصال بالنظام المعلوماتي لأي سبب من الأسباب، ويتسع ليشمل جميع الصور والمعايير في تحقيق النشاط الإجرامي، وهو انعدام حق الجاني في الاتصال بالنظام كله أو في جزء منه.

1- Devez: infraction en matière informatique, J.C.P 1988, art 462-2- a 462-9, No.41.
2- د. عمر الفاروق الحسيني – المرجع السابق – ص127.
3- Tappolet: la fraude informatique, Rêve. inter. Crim. et Pol. techn. 1988.p.351
4- د. هشام رستم – المرجع السابق – ص250.
5- Garsain (R.): informatique (Fraude informatique) Dalloz 1989.No101.p13.

ثانيا – الركن المعنوي:

يشترط في هذه الجريمة توافر القصد الجنائي المتمثل في علم الجاني أن يقوم بعمل اتصال غير مشروع وغير مسموح له القيام به مع نظام معلوماتي خاص بالغير. واتجاه إرادته إلى إقامة هذا الاتصال غير المشروع بالنظام الآلي لمعالجة المعلومات، فإذا تم هذا السلوك بدون توافر قصد الدخول الاحتيالي للنظام المعلوماتي فإن هذه الجريمة لا تتوافر لعدم تحقق القصد الجنائي، ولكن من الممكن أن تحقق قصدًا جنائيًا آخر خاصًا بجريمة البقاء في نظام معلوماتي غير مسموح له الدخول عليه. وتقدير توافر القصد الجنائي مسألة موضوعية ويقرها قاضي الموضوع على ضوء الوقائع الثابتة، ولا يتطلب المشرع توافر قصد خاص في تلك الجريمة بل يشترط توافر القصد الجنائي العام.

الدخول الاحتيالي للنظام المعلوماتي صور متعددة منها:

1- الدخول عن طريق استخدام ما يطلق عليه فيروس حصان طروادة بحيث يتمكن الجاني من إدخال هذا البرنامج إلى النظام المعلوماتي الذي يقوم بدوره بالتجسس على المعلومات، وهو فيروس يخترق النظم التقنية ويستغل نقاط الضعف فيها لإزالة التعليمات الخاصة بالسيطرة على المعلومات داخل الجهاز.

2- انتحال الشخصية بالتخفي، باستعمال حقد الولوج لشخص آخر باستخدام الشفرة الخاصة به[1].

3- جريمة الإبقاء على اتصال تم بطريق الخطأ.

يتطلب المشرع الفرنسي في هذا الفعل توافر الغش، وتتحقق عند توافر نية البقاء في الاتصال غير المشروع.

أولا – الركن المادي:

نشاط إيجابي يتمثل في الامتناع عن الخروج من الاتصال الذي تم بنظام معلوماتي بطريق الخطأ، فالمشرع حين فرض عقابًا على هذا الفعل فإنه فرض على الشخص الذي تم

1- Devze: Op. Cit.p.6.no.45.

معه هذا الاتصال أن يقوم بقطعه والخروج منه[1]. وقد يأخذ البقاء غير المشروع بالنظام المعلوماتي صورًا عديدة، منها تجاوز الوقت المسموح له للبقاء داخل النظام أو البقاء في التعامل مع النظام، رغم انتهاء عقد المستخدم وعدم تجديده. ويرى جانب من الفقه أن هذه الجريمة تعتبر صورة من صور نقل أو تعديل الحيازة بصورة غير مشروعة[2].

ثانيا – الركن المعنوي:

أن يتحقق عنصرا العلم والإرادة، وذلك بعلم الجاني أنه موجود بنظام معلوماتي غير مسموح له الدخول إليه والذي تم بالخطأ، واتجاه نتيجة إلى الإبقاء على هذا الاتصال والاستمرار فيه.

إلا أنه إذا حاول الشخص قطع الاتصال ولكنه فشل لسبب فني يجهله، إما لوجود نظام أمني لا يسمح في حالة الدخول الخطأ إلا بإجراءات محدودة أو نتيجة استخدام الاتصال التلفوني الذي قد يحتاج وقتا لتحميل أمر الإنهاء، عندئذ ينتفي توافر القصد الجنائي، ويتعين على المحكمة التأكد من صحته عند إثارته.

الإتلاف غير العمدي للمعلومات:

تناول المشرع في الفقرة الثانية من المادة 462-2 تجريم الدخول إلى النظام أو البقاء فيه بطريقة الغش إذا أدى ذلك إلى الإلغاء أو تغيير أو تشويه البيانات المخزنة بالنظام[3]. وقد اعتبر جانب من الفقه أنها من قبيل الجرائم المستقلة ذات النتيجة أو هو تجريم ثنائي من المشرع[4]، ويرى اتجاه آخر أنها من الظروف المشددة، لأنه يفترض

1- د. عمر الفاروق الحسيني – المرجع السابق – ص129-130.

Garsain: Op. Cit. No. 1109 Croze: l'apport du droit pénal 'a loi la théorie du la fraudé de l'informatique c'a propos de la loi no 88-19 du Janvier 1988 relative 'a la fraude informatique, J.C.P 1988 ,13, chamoux: la loi Sun la Froude informatique de nouvelles in criminalisons , J.C.P 1988. 13. no.7

2- Croz , op. Cit. No 11 , Gamin: op.cit. no. 4

3- Deveze: op.cit. no. 48.p.6

4- Buffelan: la répression de la fraudé informatique de novelles in criminalisons, J.C.P. 13.P.10 , chamoux , Op.cit. No.8

لتطبيق هذه الجريمة أن يكون الفاعل مرتكبا لجريمة الدخول إلى النظام معلوماتي أو البقاء فيه بطريقة الغش، الأمر الذي يجعلها تتمتع بذاتية مستقلة عن الجريمة السابقة، في حين أن الجريمة ذات النتيجة يكون لها استقلالية إجرامية[1]، وهو ظرف عيني في حالة الاشتراك يمتد إلى كافة الشركاء في الجريمة[2].

أولا – الركن المادي:

تقع الجريمة بواسطة إلغاء أو تغيير أو تشويه للبيانات المخزنة في النظام المعلوماتي ويقصد بالإلغاء إزالة المعلومات الموجودة داخل النظام المعلوماتي، ويقصد بالتغيير إحداث تعديلات في المعلومات مما يجعلها مخالفة للمدونة قبلا، والتشويه هو القيام بتعريف المعلومات بحيث تصبح غير مطابقة جزئيا للمعلومات الأصلية كما يشترط توافر رابطة السببية بين النشاط الإجرامي وحدوث الإلغاء أو التغيير أو التشويه[3].

ثانيا – الركن المعنوي:

والمستفاد من النص أن الجريمة تتحقق ولو بطريق الخطأ، وبالتالي فإن مجرد ارتكاب الفعل المادي يعد كافيا لوقوع الجريمة.

الإتلاف العمدي لإدارة النظام المعلوماتي:

يعاقب المشرع الفرنسي في المادة 3/462 " كل من يقوم بالتعطيل أو الإفساد العمدي ودون مراعاة لحقوق الآخرين تشغيل نظام المعالجة الآلية للبيانات يعاقب......".

أولا – الركن المادي:

يتكون النشاط الإجرامي في هذه الجريمة من نوعين من الأنشطة الإجرامية، وهي تعطيل أو إفساد تشغيل النظام الآلي لمعالجة البيانات، وقد استهدف المشرع الفرنسي من

1- Lucas de Leyssac: Commentate de la loi du 5 Jan. 1988 R.D, informatique télécom, 1988.p.22

2- Stepain , levaseur et Bouloc: Droit pénal général , 13 éd , 1987. No 279.

3- Deveze , op.cit , no.49 , Lucas de lrgymac: fraude informatique , Rêv.droit.Op.cit. P.23.

خلال نص على تجريم تلك الأنشطة الإجرامية إلى حماية النظام المعلوماتي، وطريقة عمله. وذلك من خلال إدخال تعليمات طفيلية تشويشية على النظام المعلوماتي مما يؤدي إلى إعاقته عن العمل، وتلك التعليمات الطفيلية هي الفيروسات المنطقية، ذلك أنها تدخل بصورة منطقية إلى النظام المعلوماتي فتؤثر على المعلومات المخزنه فيه[1]. وكذا التأثير على النظام من حيث إدارته واستغلاله بغرض الحصول على منافع معينة، وهو الأمر الذي يجعل هذا الفعل خاضعا للتجريم وفقا لهذا النص[2].

ويقصد بمصطلح الإعاقة أو الإفساد للنظام المعلوماتي، أي تغيير في البرنامج يؤدي إلى إحداث نتائج أخرى غير متوقعة، وهو ما يدخل ضمن نطاق استخدام الفيروسات مثل: حصان طروادة والقنابل الفيروسية المنطقية إلى غير ذلك من أنواع الفيروسات التي تؤثر على إدارة النظام المعلوماتي بإحداث تغييرات جوهرية بما يؤثر على البرامج في أدائها وظائفها المختلفة[3]. ولتحديد المعاني الواردة في النص ينبغي الرجوع إلى معاني المفردات، والإفساد يعني تشويه أداء الحاسب لعمله وجعله غير صالح للاستعمال، فوفق هذا المعنى ينصب على المكونات المادية وغير المادية للنظام المعلوماتي[4].

وبالنسبة لمصطلح التعطيل فهو لغة القيد الذي يربط به الحيوان للحد من حركته، واصطلاحا القيد من حركته، واصطلاحا فهو يعني تقييد حركة الحاسب الآلي على نحو يصيب نظام المعالجة الآلية للبيانات بالشلل المؤقت[5]. والإعاقة نوعان مادية وذهنية، وتتوافر في حالة وجود حائل مادي يحول دون أن يسير النظام في عمله المعتاد، ومن أمثلة ذلك التعطيل التعرض للمكونات المادية الخاصة بجهاز الكومبيوتر Hard ware ، وتتوافر

1- Gramain: op.cit.p.158.
2- Buffelan , op.cit.p.102.
3- Deveze, op.cit.p.9.
4 – د. عفيفي كامل عفيفي – جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية – المرجع السابق ص192-193.
5- د. محمد سامي الشوا – المرجع السابق – ص200، د. أيمن فكري – مرجع سابق – ص 210 .

الثانية في الإعاقة الذهنية التي تكون على جانب كبير من الدقه نظرا للطبيعة الفنية للوسائل المستخدمة في إحداثها، والتي تتمثل في القنابل المنطقية والفيروسات[1].

ثانيا – الركن المعنوي:

انتقد اتجاه في الفقه لصياغة المشرع لعبارة ازدراء حقوق الغير العديد من الصعوبات الناتجة من غموضها، وهل يقصد به وقوع الضرر، وهل الضرر الحالي أم الاحتمالي، ويرى جانب من الفقه أن المشرع اشترط الضرر[2]. واتجه جانب من الفقه على أن القصد الخاص يتمثل في قصد الإضرار بالغير إلى جانب العلم والإدارة المتطلب في القصد العام، وذلك على ضوء ما ورد بنص القانون، وتطلبه توافر الفعل مع ازدراء حقوق الغير[3].

المبحث الثالث
الإتلاف العمدي للبيانات

نص المشرع الفرنسي في المادة 462–4 على أن كل: من يقوم عن قصد – مزدريا بحقوق الغير – مباشرة أو غير مباشرة – بإدخال بيانات بداخل نظام للمعالجة الآلية مدة تترواح ما بين ثلاثة أشهر إلى ثلاث سنوات وبغرامة ما بين 2000 يورو إلى 500000 يورو أو بإحدى هاتين العقوبتين".

المطلب الأول- الفروق الجوهرية بين الإتلاف العمدي وغير العمدي للبيانات:

بالنظر إلى الأفعال التي تضمنتها المادة، يتبادر إلى الذهن أنها قريبة إلى جريمة الإضرار العمدي بإدارة النظام المعلوماتي الوارد بالمادة 462–3 فإن المشرع قد جعل هذا الالتباس قائما، وسنعرض للتجريم في المادة السابقة مع إبراز التمايز في تطبيق النصين السالفين:

1– د. محمد سامي الشوا – المرجع السابق – ص 201، د. عفيفي كامل عفيفي – المرجع السابق – ص192.

2- Buffelan: les nouveaux délits informatiques expertise , 1988, p. 101.

3- Pradel (J.): les infractions relatives 'a L'informatique R.D.P.C, 1990.p.874.

أولا – معيار التمييز:

رأى اتجاه في الفقه بأن نص المادة 463–3 أن يكون نوع التغيير من حيث كونه تم بطريقة – معنوية أو بصورة مادية، الأمر الذي يجب أن يأخذ بظاهر النص، وإن التغيير المقصود هو التغيير الجزئي، وأن التغيير الكلي يخضع لنص المادة 462–4 حيث إنّ التشديد في العقوبة المذكورة في النص، يدل على وجود خطورة إجرامية[1].

الركن المادي:

فعل إحداث تغيير في المعلومات الواردة في نص المادة 462–4 هي التغيير بما يؤدي إلى عمليات تشويشية على عمل الجهاز، وأن يتم التخريب بصورة تتسم بقدر من الجسامة لتتناسب مع التشديد الذي أورده المشرع.

الركن المعنوي:

يتمثل ذلك في توافر عنصري العلم والإرادة المتجه إلى القيام بتلك الأفعال، ويتطلب النص كذلك نية الإضرار بالغير، وذلك بذكر لفظ "إزدراء لحقوق الغير" الأمر الذي يجعل العلم غير معاقب عليه إلا بتوافر القصد الخاص[2].

المطلب الثاني - التجريم المعاصر في قانون العقوبات الفرنسي:

اتجه المشرع الفرنسي في قانون العقوبات الحديث إحكام الحماية المعلوماتية، وتناول هذه الحماية بطريقة غير مباشرة من الإتلاف المعلوماتي في نص المادة 323–1 ق.ع.ف، والحماية المباشرة بالمادة 323–3,2 [3].

موقف الاتفاقية الأوربية:

أبرمت الاتفاقية الأوربية لمكافحة جرائم المعلوماتية في مدينة بودابست في سبتمبر 2001، وتم النص على تجريم الولوج غير القانوني بالمادة الثانية من الاتفاقية: يجب على

1- Philippe Rose: La criminalité informatique, puff, 1 éd ,1988.P.61.
2- Devez , Infraction en métiers , Op. Cit.p.1
3- د. عمر الفاروق الحسيني – المرجع السابق – ص122–123

كل طرف أن يتبنى التدابير التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقا لقانونه الداخلي، الولوج العمدي لكل الجهاز الحاسب أو جزئه بدون حق ويشمل التجريم نشر أو بث فيروسات لا مجرد حيازتها فقط، وتجريم هذا الفعل يمتد على مجرد بث الفيروسات دون اشتراط تحقق الضرر، وهناك من التشريعات ما يشترط حدوث إعاقة أنظمة الحاسبات الآلية كما هو في القانون الفيدرالي الأمريكي[1].

المبحث الرابع
الحماية غير المباشرة من الإتلاف المعلوماتي

تعاقب المادة 323-1 ق.ع.ف وذلك بالقانون الصادر في الأول من يناير 1994 وذلك لتحقيق الردع العام، ونص على أن "يعاقب على الدخول بطريقة الغش أو التدليس على نظام معالجة البيانات أو إبقاء الاتصال بطريقة غير مشروعة بالحبس لمدة سنتين وبغرامة 30 ألف يورو، وتكون العقوبة الحبس لمدة ثلاث سنوات وغرامة 45 ألف يورو "إذا ترتب على نشاط الجاني إلغاء أو تعديل البيانات الموجودة بالنظام أو تعديل تشغيل النظام"[2].

وقد تضمن هذا النص القانوني تجريم فعلين ونتيجة، أما الفعل الأول فهو الولوج غير المشروع للنظام المعلوماتي، والفعل الثاني يتمثل في الإبقاء على الاتصال أو الولوج بطريقة الخطأ[3]، ونتيجة تتمثل في تشديد المشرع للعقاب، إذا حدث إضرار بالمعلومات أو البرامج التي يحتوي عليها النظام المعلوماتي من خلال إلغاء أو تعديل البيانات المخزنة بالنظام أو تعديل تشغيل النظام.

المطلب الأول- تجريم الولوج غير المشروع للنظام المعلوماتي:

رأى بعض الفقه أن التجريم الوارد في نص المادة 323-1 ق.ع.ف تحكم الحماية من خلال تشديد العقوبة على الولوج إلى أنظمة الاتصالات وذلك لاعتماد الإتلاف

1- Silber Ulrich: computer crime and other crimes against information , I.R.P.L. 1993.Vol.64.P.80.

2- د. عمر محمد أبو بكر يونس – مرجع سابق – ص237.

3- Bain bridge David Hacking: The un authorized access of computer system , the legal implications , M.L.Rev.March 1989 ,Vol. 52.p.137.

المعلوماتي على تلك الناحية الفنية[1]. ولما كان مستودع سر الإنسان لم يعد مقتصرا عل تلك الصور التقليدية التي كان عليها في السابق بل انتقل إلى نظم المعالجة الآلية للبيانات سواء أكان على مستوى الفرد أم المجتمع بهيئاته ومؤسساته، وفي تلك الحال فإن انتهاكها من قبل أحد الأشخاص يؤدي إلى الاطلاع على تلك الأسرار، وتهديد المعلومات بخطر الإتلاف أو السرقة، ولذلك ظهرت الحاجة إلى حمايتها من خلال تجريم الولوج غير المشروع لتلك المعلومات.

مفهوم الدخول غير المشروع للنظام المعلوماتي:

يعرف الدخول غير المشروع أو الولوج أو الاختراق أو الانتهاك للنظام المعلوماتي، بأنه الولوج غير المصرح به أو بشكل غير مشروع إلى نظام معالجة البيانات باستخدام الحاسوب. ويتجه جانب من الفقه بأن الدخول غير المشروع إلى النظام المعلوماتي بالوصول إلى المعلومات والبيانات المخزنة داخل النظام المعلوماتي ودون رضاء من المسؤول عن هذا النظام أو المعلومات التي تحتوى عليها.

وفي اتجاه آخر بأنه إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مصرح له باستخدامه والدخول إليه، للوصول إلى المعلومات والبيانات المخزنة بداخله للاطلاع عليها أو لمجرد التسلية، أو لإشباع الشعور بالنجاح في اختراق الحاسب الآلي على الرغم من الاحتياطات التقنية التي يحتوي عليها نظامه. ينشأ النشاط الإيجابي من جانب الجاني ويتمثل في الدخول في الاتصال بطريقة الغش مع النظام الآلي لمعالجة المعلومات كلها أو جزء منها، ويقتضي هذا الأمر أن نستوضح عنصرين هامين وهما: الدخول الاحتياطي أو بأية صورة، والنظام المعلوماتي أو نظام المعالجة الآلية للبيانات.

المطلب الثاني - مفهوم نظام المعالجة الآلية للبيانات:

طبقا لنص القانون، فإن نظام المعالجة الآلية للبيانات يعدّ محل الجريمة، وقد ورد تعريف نظام المعالجة للبيانات بأنه "مجموعة الأشياء المادية والمناهج والبرامج المرتبطة

1- European committee on crime problems , Strasbourg 1990.p.49.

بالحاسب الآلي والمختصة باستقبال ومعالجة ومعاملة البيانات"[1]. ونظرا للانتقادات الموجهة للتعريف، فقد حاول البرلمان الفرنسي أن يضع تعريفًا للنظام الآلي لمعالجة البيانات، وذلك لوضع حد للخلاف القضائي بالنسبة للأحكام القضائية وعرفه بأنه "مجموعة وحدات المعالجة أو الذاكرة أو البيانات أو نظام الدخول أو الخروج أو وحدات الاتصال التي تساعد على تحقيق النتيجة المطلوبة، وتكون موضوعًا للحماية بنظام الأمن"[2].

وباستعراض التعريف اللغوي نجد أنّ النظام هو عنصر مركب تم تشكيله من عدة وحدات متميزة متصلة مع بعضها البعض بواسطة عدد من العلاقات التي تنشأ لتحقيق التفاهم والترابط بين هذه المكونات أو الوحدات المختلفة وهو ما يتفق مع ما يتجه إلى أنّ النظام يتكون من عنصرين: الأول جماعية المكونات الداخلة في النظام، والثاني وجود شبكة من الاتصالات بين هذه العناصر[3]. وهو ما نجده يتفق مع ما ذهب إليه البرلمان الفرنسي، وقد ورد عناصر التشريع على سبيل المثال لا الحصر، ليشمل كافة التطورات الحديثة، ويدخل ضمن نطاقه الشبكات المعلوماتية، وحالات الاستخدام لبطاقات الائتمان الممغنطة، والتي يرى جانب من الفقه أن تستبعد من النظام المعلوماتي على أساس أنها إحدى عناصره[4].

وقد أورد حكم قضائي مصطلحًا مترادفا مع اصطلاح نظام المعالجة المعلوماتية باستخدام مصطلح المعالجة الأوتوماتيكية للبيانات، فقرر بأنه يقصد المعالجة لمجموعة العمليات المتحققة بواسطة الوسائل الأوتوماتيكية الخاصة بتجميع وتسجيل وإلغاء وتعديل وحفظ وإنشاء، ونسخ البيانات، وبمفهوم عام القدرة على استغلال هذه البيانات[5]. ويتجه جانب من الفقه إلى تعريف المعالجة المعلوماتية للبيانات "بأنها النتيجة النهائية أو تصور شيء ما أو ظاهرة مادية، فهي الفكرة التي تتكون عن شيء ما، أما المعلومة فتشكل محتوى

1- Garsing: op.cit.p.17.
2- Devze: op.cit.p.7.
3- Garsian (R.): Informatique, op.cit.p.10. s. (www.encyclopedia).
4- د. أحمد حسام طه – المرجع السابق – ص283.
5- Gassin: op.cit – No 74.p.10.

للبيانات، وبناء على هذا التعريف فإنه يدخل ضمن مفهوم البيانات تلك التي تكون خالصة، وتتكون من مجموعة بيانات مثل البرامج[1]. ويتجة جانب من الفقه بأنها رسالة معبر عنها في شكل يجعلها قابلة للتوصيل إلى الغير، فهي قابلة للتوصيل للغير بفضل علامة أو إشارة ويتجه جانب من الفقه إلى أنه يجب التفرقة بين المصطلحين، وهي المعالجة الآلية والمعالجة المعلوماتية واستندوا في ذلك للمعاهدة الأوربية الصادرة في 28 يناير 1981 فإن فكرة المعالجة الآلية تعد أكثر شمولا من فكرة المعالجة المعلوماتية فالمعالجة الآلية: The treatment ذات الطابع التحليلي الشامل لكل البيانات المدرجة بالنظام حيث تتقبل المعالجة للاستفهام، أو الاستدعاء وتجيب عليه بمعنى ارتكاب المعالجة على قاعدة الاستقبال والإرسال في داخل الحاسب أو النظام المعلوماتي[2].

النتائج التطبيقية لتحديد مفهوم المعالجة الآلية للبيانات:

الجرائم التي نص عليها المشرع بالقانون 323-1 لا تقع إلا إذا كانت التصرفات التي تم تجريمها غير خاضعة لنظام المعالجة الآلية للبيانات.

يشترط أن يكون نظام المعالجة الآلية للبيانات في حالة عمل بحيث يمارس وظائفه بصورة طبيعية ويترتب على ذلك أنه في حالة عدم تشغيل النظام فإنه لن يكون هناك تجريم للتصرفات الواردة على النظام[3].

- في حالة تواجد أنظمة متعددة لمعالجة البيانات التي ستدخل الحاسب الآلي، فإن الحماية المقررة لشخص لاستخدام أحد هذه الأنظمة لا لتغطية الحق في التعامل مع الأنظمة الأخرى بحيث أنه ترتب على هذا التعامل حدوث أضرار مع توافر التعمد لدى هذا الشخص فإنه يخضع لتلك النصوص التجريمية المعاقب عليها.
- إنّ اشتراط وقوع الفعل على نظام المعالجة البيانات يجعل الفعل الذي يقع على وسائل الاتصال غير المعاقب عليه استنادا إلى أنّ قصد المشرع يستهدف الأفعال التي تقع على النظم المعلوماتية[1].

1- د.عمر حسبو – المرجع السابق – ص 30.

2- Buffelan: la repression de la fraude informatique, exportés, Ferrié. p.58.

3- Chamoux: la loi sun la fraude informatique, Op.cit. No.10.

وقد استقر مفهوم المعالجة الآلية للبيانات القانون الفرنسي الحديث، بالقانون الصادر عام 1994م في المادة 323-1 على الأخذ بالمفهوم الموسع بنظام المعالجة الآلية للبيانات، فالمادة تجرم الدخول إلى كل النظام الآلي أو بعضه لمعالجة البيانات كعنصر لقيام الجريمة، فالجريمة لا تقوم بالدخول إلى أيّ جزء يحتوي على معلومات متى كان بمعزل عن نظام المعالجة الآلية للمعلومات(2).

مفهوم الدخول الاحتياطي أو التدليس:

نص المشرع المادة 323-1 على تجريم فعل الدخول غير المشروع وفرق بينه وبين فعل البقاء غير المشروع بالنظام المعلوماتي، ويمكن القول أن البقاء غير المشروع هي جريمة مستمرة على اعتبار أن فعل الدخول تخطى المسموح به، أما الدخول غير المشروع فهي جريمة وقتية وسنعرض لذلك فيما يلي:

أ- **مفهوم عدم التصريح بالدخول:** إنّ مجرد الدخول إلى النظام المعلوماتي لا يشكل فعلاً غير مشروع إلا إذا كان هذا الفعل قد تم بدون وجود تصريح أو سبب قانوني يعطي السلطة للشخص في الدخول إلى النظام المعلوماتي، ولا يثير حالات الدخول للنظام المعلوماتي من الغير(3)، ولكن في حالة الدخول المصرح به فإنه يخضع لنص آخر إذا كان البقاء لمدة أطول من المدة المسموح له بها.

ب - **مدى اشتراط توافر الوسائل التقنية والحماية الجنائية:** تطلب اتجاه غالب في الفقه إلى عدم تطلب توافر حماية أمنية للنظام المعلوماتي كشرط لإصباغ الحماية الجنائية ضد انتهاك النظام المعلوماتي(4)، ويرى اتجاه آخر أنه لا يلزم توافر نظم أمنية للنظام المعلوماتي حتى يتمتع بالحماية الجنائية(5).

1- Croze: op. cit.No.17.

2- Lucas Leyssac: Fraude informatique ,loi du sjanvier 1988 Rev. Dr.inform. telecoms. 1988. no 2.Croze: op.cit.J.C.P.I.3

3- Stravropolou Maria , Read chirs: computer crime The new Greek law, C.L.P. 1989 ,p. 215

4- Buffelan: op.cit. p. 58 , Deveze: infraction en matie're , op. cit. p. 9 ,

5- Jérôme Huet et Herbert Maisi droit de l'informatique et des télécommunications de lois constitution Nelles de la législation et de l'administration général de la

ونرى أن التعامل مع نظام معالجة الآلية كبيئة افتراضية يقتضي أن تكون هناك وسائل حماية أمنية حتى لا يكون النظام متاحا للكافة، وبالتالي فإنه يمكن محاسبة من يقوم بالولوج إليه كما يمكن إضافة الأسباب الآتية يمكن أن نوردها فيما يلي:

1- إنّ القانون يفترض في المال محل الاعتداء أن يكون محددا وواضح المعالم بالنسبة للكافة، وفي حالة وجود نزاع عليه أو سلطة في التعامل مع المال، فإنه ركن من أركان الجريمة ينتفي، وبالتالي لا تقع الجريمة، كما أنه من المنطق والقانون يوجب أن تكون هناك من الإجراءات التقنية ما يتيح للأفراد العلم بالمنع المفروض عليهم بالنسبة للولوج إلى تلك النظم.
2- إنه في حالة عدم اشتراط توافر الإجراءات التقنية فإنّ التعامل البرمجي مع النظم المعلوماتية من خلال البرامج وأدوات البحث الإلكترونية التي تقوم بها مواقع البحث، سوف يوقع الكثير من الأفراد تحت طائلة التجريم، ثم العقوبة.
3- فرض المشرع على الجهات التي تتعامل مع البيانات الخاصة بالأفراد أن تكفل لها الحماية التقنية الملائمة لها ضد الانتهاك أو الإطلاع من قبل الأشخاص غير المصرح لهم وفرض عقوبة على الجهات التي لا تلتزم بحماية البيانات[1].

البقاء بطريقة الغش في نظام المعالجة الآلية:

ويعرف هذا السلوك بأنه "مشاركة ذات سيطرة من المخترق على عمليات الحاسب الآلي إلى النظام المعلوماتي، أي؛ البقاء في نظام المعالجة الآلية للبيانات[2] جريمة البقاء غير المشروع في النظام المعلوماتي تفترض اختلاس وقت النظام وتتخذ صورة الجريمة

république Sun la proposition de M. Godfrain relative 'a fraude informatique No 744.p.13

1- د. هشام فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط طـ1994 ص134، د. عمر الوقاد – الحماية الجنائية للمعلومات – مجلة روح القوانين – حقوق طنطا – إبريل 1998 ص 52، د. عوض محمد – دراسات في الفقه الجنائي الإسلامي – دار المطبوعات الجامعية – الإسكندرية 1998 ص 91.

2- Vergutch (P.): Op.Cit.p.197.

المستمرة[1] ويأخذ فعل البقاء صورًا متعددة منها تجاوز الوقت المسموح به للبقاء داخل النظام، أو البقاء رغم تجديد عقد الجاني، وفعل البقاء من الممكن أن يكون نشاط سلبيا أو إيجابيا[2].

ويرى اتجاه أن نص المادة 323-1 يتطلب أن يكون الدخول أو البقاء بالنظام المعلوماتي تم بطريقة الغش أو التدليس، وبناء عليه إذا كانت قاعدة البيانات مفتوحة، للجمهور كان الدخول، ومع ذلك يكون البقاء منها بعدم المشرعية[3].

جريمة الدخول بطريق الغش في نظام معلوماتي:

استخدم المشرع الفرنسي المصطلح Fraud Linesmen وتعني الغش وذهب غالبية الفقه أن ما يتطلب المشرع في تلك الجريمة والإرادة، أي؛ القصد الجنائي العام[4]. ويشترط في القصد الجنائي أن يتعاصر مع النشاط الإجرامي في جريمة الدخول بطريق الغش إلى نظام المعالجة الآلية للبيانات، فإذا لم يتحقق القصد الجنائي وقت الدخول وتوافر لاحقا، وجريمة البقاء غير المشروع هي تلك التي تتحقق وتتوافر أركانها في حق الجاني والتي تأخذ في تلك الحالة عنصر العلم وقت أن توافر لدى الجاني بأن وجوده في هذا النظام غير المشروع نتيجة إرادته إلى الاستمرار في هذا الاتصال الذي تم بطريق الغش.

ولما لم يشترط المشرع في حدوث النتائج التي رتب عليها تشديد العقاب بالمادة 323-1 أن يتم إحداث تلك النتائج بطريق الغش أو أيا من المصطلحات التي تدل على

1- د. علي عبد القادر القهوجي – الحماية الجنائية للبيانات المعالجة إلكترونيا – بحث مقدم لمؤتمرات القانون والكومبيوتر والإنترنت – كلية والقانون الإمارات العربية المتحدة – 2000 ص19.

2- Verqutch Pascal: op.cit.p.211, Bainbridge David: introduction to computer law, 4ed Longman 2000. p.314.

3 –Gabriel Roujou de Boube'e , Bernard Bouloc , Francillon yever Mayaud ,op.cit.pp. 611 ets , Hansen Ann C: Criminal law theft use of computer Services , state V. Megraw , W.E.l. rev. vol. 7.p.823 , Deveze: Atteintes aux systèmes, op.cit. No.44 , Vivant (M.) et Stanc (Ch.): la droit de le informatique , 1989 No.2479.p.1504.

4- د. نائلة عادل فريد قورة – المرجع السابق – ص378، د. مدحت رمضان – المرجع السابق – ص 53.

تتطلبه لتوافر القصد العمدي في إحداث تلك النتيجة، وهو الأمر الذي وجد معه الفقه، إنّ تلك الجريمة تقع بطريق الخطأ ولا يتطلب المشرع فيها توافر القصد الجنائي العمدي، بحيث أن الخطأ يعد كافيا لقيام الجريمة، ومن ثم فإن هذه الجريمة تعد من جرائم الإهمال، وبالتالي ارتكاب الفعل المادي يعد كافيا لقيام الجريمة إلا إذا استطاع الجاني إثبات حدوث قوة قاهرية.

الجرائم المشددة للإتلاف المعلوماتي:

حرص المشرع الفرنسي على الإبقاء على الاهتمام بالحماية الجنائية من الإتلاف المعلوماتي بأشكاله المختلفة من خلال تخصيص فقرتين بالمادة 323 من القانون الجنائي الحديث عما كان عليه المال بالقانون رقم 88/19، وتعديلاته بالقانون 1994، وذلك بتعديل في الصياغة وتشديد في العقاب.

ونص المشرع في المادة 323–2 من قانون العقوبات الفرنسي الحديث على أن يعاقب كل من يقوم "بتعطيل أو إفساد تشغيل نظام المعالجة الآلية للبيانات بالحبس لمدة خمس سنوات وغرامة قدرها 75 ألف يورو"[1]. ونص المادة 323–3 على معاقبة كل من يقوم "بإدخال بيانات بطريقة الغش في نظام المعالجة الآلية للبيانات أو محوها أو التعديل بطريق الغش للبيانات التي يحتوي عليها بالحبس لمدة خمس سنوات وبغرامة 75 ألف يورو"[2].

الركن المادي:

أ– جريمة إعاقة أو إفساد نظام التشغيل بالمادة 323–2:

وتقع هذه الجريمة بكل فعل يتسبب في تباطؤ أو إرباك عمل نظام المعالجة الآلية للبيانات، ومن ثم ينتج عن ذلك تغيير في حالة عمل النظام[3].

1- S.(www.legifrance.gouv.fr).

2- S.(www.legifrance.gouv.fr) ،Bibent Michel: le droit du traitement de l'information, Nathan, 2000 , PP.120-121.

3– د. أحمد حسام طه تمام – المرجع السابق – ص351.

ويتضح من خلال المصطلحات المستخدمة بنص المادة 323-2 أنها تشمل كل فعل من شأنه إرباك عمل نظام المعالجة الآلية للبيانات، ويستوي أن يؤدي نشاط الجاني إلى توقف نظام العمل بصورة دائمة أو مؤقتة أو أن يستخدم الجاني في ارتكاب الجريمة أو أي وسيلة من شأنها أن تعوق سير النظام كالاعتداء المادي على النظام أو نشر فيروسات في النظام المعلوماتي(1).

ب- جريمة إتلاف المعلومات:

نص المشرع الفرنسي بالمادة 323-3 على تجريم أيّ نشاط يترتب عليه إتلاف المعلومات المخزنة بالنظام المعلوماتي وعاقب على إدخال بيانات في النظام للمعالجة الآلية للمعلومات أو إلغاء أو تعديل البيانات المخزنة في النظام المعلوماتي. وعلى ذلك فالمشرع الفرنسي يعاقب على إتلاف المعلومة المخزنة في ذاكرة الحاسب الآلي أو على وسيط التخزين المعلوماتي، حيث يؤدي إدخال البيانات إلى شغل الذاكرة في النظام المعلوماتي بالكامل فيعجز عن التعامل مع هذه المعطيات بمعالجتها أو باستخداجها مطبوعة على أوراق، أو محو المعلومات أو تعديلها(2).

وقد طبقت محكمة النقض الفرنسية المادة 323-3 على قيام أحد الأشخاص بتعديل وإلغاء معلومات تتعلق باللوائح المطبقة بإحدى الشركات بطريقة العمد، وقد أقرت المحكمة بأنه ليس من اللازم أن تكون هذه التعديلات أو الإلغاءات تم ارتكابها بواسطة شخص ليس له حق الدخول في النظام ولا يشترط أن يتوافر لدى الجاني نية الإضرار، وبناء على ذلك فإن قيام الشخص بتعديل البيانات التي سبق وأن قام بتسجيلها بطريقة نهائية على نظام آلي للمحاسبة كان يقوم بالإشراف عليه(3).

1- Alian Bensoussan: le commerce électronique, aspects Juridiques, Hermès, 1988, Henri Alterman , le fraude informatique , op.cit.p.53.

2- د. جميل عبد الباقي – الإنترنت والقانون الجنائي – دار الفكر العربي 2001 ص 63، د. هدى قشقوش – الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني – جامعة الإمارات العربية المتحدة – 1-3 مايو 2000.

3- Cass.Crim, 8dec, 1999, Bull No.296. S.(www.legalis.net).

ويجب مراعاة التمييز بين الإتلاف المعلوماتي والتزوير المعلوماتي، ويهدف بإحداث الإتلاف أو التغيير أو التخريب، أو الإضرار بالنظام أو المعلومات دون أن يكون قصد الجاني متجها إلى استغلال أو استخدام تلك المعلومات في شيء ما، بعكس التغيير أو التلاعب في المحرر المعلوماتي الذي يهدف الجاني من خلاله إحداث تغيير في حقيقة المحرر المعلوماتي.

ثانيا – الركن المعنوي:

تطلب المشرع توافر القصد الجنائي الذي يتحقق بتوافر العلم لدى الجاني بأنه يقوم بأحد الأفعال التي جرمها النص القانوني سواء أكان بإتلاف أم إعاقة النظام المعلوماتي عن أداء وظائفه، وأن تتجه إرادة الجاني إلى ارتكاب الفعل وتحقيق نتيجة[1]. وقد ارتبطت جريمة الإتلاف وإعاقة النظام المعلوماتي غير العمدية بالدخول أو البقاء غير المصرح به في النظام المعلوماتي، فالمادة 323-1 تجرم الدخول أو البقاء بطريق الغش في النظام المعلوماتي وتشديد العقاب متى نتج عنه محو أو تعديل للمعلومات أو إفساد للنظام المعلوماتي[2].

الخاتمة

تبرز أهمية مكافحة جرائم المعلوماتية بما تمثله هذه التقنيات في حياة الناس اليوم، فلا تكاد تجد متخصصاً أو غير متخصص أو منشأة تجارية أو غير تجارية إلا ولها تعامل واضح وبارز مع تقنية المعلومات. وسنعرض لأهم التوصيات لمكافحة الإتلاف المعلوماتي، ومدى كفاية الحماية المباشرة أو غير المباشرة فيما يلي:

1- د. علي عبد القادر القهوجي – المرجع السابق – ص378، د. نائلة عادل قورة – المرجع السابق – ص227.

Devez: Atteinte aux Systems de traitement automatise' de Donnés, op.cit.No.60.p.13.

2- د. محمد سامى الشوا – المرجع السابق – ص202.

1- ضرورة تجريم الولوج في حد ذاته، وهو ما يطلق عليه الحماية غير المباشرة للمعلومات وليس فقط الاكتفاء بتجريم فعل الإتلاف، وذلك كما جرمه المشرع الفرنسي في قانون العقوبات.
2- ضرورة تشديد العقوبات والغرامات حال ارتكاب جريمة الإتلاف المعلوماتي أو حتى مجرد الولوج إلى نظم المعالجة المعلوماتية، والمساواة في ذلك بين الاعتداء على تلك الخاصة بالجهات الحكومية أو الخاصة تأمينا لحركة التجارة الإلكترونية أو المعلومات الخاصة.
3- المساواة في العقوبة بين الجريمة العمدية وغير العمدية، حماية من الاعتداء على النظم المعلوماتية، وبخاصة على المعلومات المودعة في بنوك المعلومات.
4- أن يتم إفراد قانون خاص لتجريم كافة صور الاعتداء على المعلوماتية، وتوجيه العناية للحماية غير المباشرة للمعلوماتية.
5- أن يتم عقد الاتفاقيات الثنائية للتسليم في جرائم الإتلاف المعلوماتي، وأن لا تخضع جرائم الإتلاف المعلوماتي للتقادم.
6- بقيت مسألة المنتجون لبرامج الحاسب الآلي والمصممون لهذه البرامج لتدمير البرنامج في حال نسخ البرامج بطريقة غير مأذون فيها.

المراجع

المصادر الشرعية:

- أبو عبد الله محمد بن إسماعيل البخاري، صحيح البخاري، دار الدعوة، ودار سحنون إستنبول، الطبعة الثانية، 1413هـ.
- أبو الحسن مسلم بن الحجاج، صحيح مسلم، دار الدعوة، ودار سحنون إستنبول، الطبعة الثانية، 1413هـ.
- أبو الفضل جمال الدين محمد بن مكرم بن منظور المصري، لسان العرب، دار صادر بيروت – لبنان1420هـ.
- الحافظ أحمد بن علي بن حجر العسقلاني، تحقيق / أبو الأقبال صفر أحمد، تقريب التهذيب، دار العالمية، 1412هـ.

الكتب والمؤلفات:

- د/ هدى حامد قشقوش، الإتلاف العمدي لبرامج وبيانات الحاسب الآلي الإلكتروني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام 2000م.
- نظام يعقوبي، الأحكام الفقهية للتعامل بالإنترنت، ندوة البركة التاسعة عشرة للاقتصاد الإسلامي مكة المكرمة، رمضان، 1421هـ.
- عبد الرحمن بن عبد الله السند، الأطر العامة لأحكام تقنية المعلومات، ورقة عمل مقدمة إلى ورشة العمل الثالثة في أحكام المعلوماتية، الخطة الوطنية لتقنية المعلومات الرياض، 1423/10/19هـ.
- د. فهد بن عبد الله اللحيدان، الإنترنت (شبكة المعلومات العالمية)، الطبعة الأولى، 1417هـ.
- جوني آرليفن، ترجمة/ فوزي عبد المنعم، الإنترنت للمبتدئين، مكتبة جرير، الرياض، الطبعة الأولى، 1997م.
- صلاح حامد رمضان علي، الإنترنت والتجارة الإلكترونية، نشرة شركة الراجحي المصرفية للاستثمار ذو الحجة، 1421هـ.
- الدكتور/ أحمد عبد الكريم سلامة، الإنترنت والقانون الدولي الخاص: فراق أم تلاق؟، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، عام 2000م.
- د/ خالد بن عبد العزيز الغنيم، و د/ عبد الرحمن بن سعد الجضعي، البرامج الحرة – حقيقة الثورة الرقمية القادمة، الطبعة الأولى، 2002م
- محمد بن عبد الرحمن الشارخ، تأثير حماية الحقوق الفكرية على الجوانب الاقتصادية، بحث مقدم إلى ملتقى حماية الحقوق الفكرية المعقود بالكلية التقنية بالرياض، بتاريخ 16 / 11 / 1420هـ.
- د/ محمد بن عبد الله القاسم، د/ رشيد الزهراني، عبد الرحمن بن عبد الله السند، عاطف العمري، تجارب الدول في مجال أحكام في المعلوماتية، مشروع الخطة الوطنية لتقنية المعلومات، 1423هـ.
- روب سميس، مارك سبيكر، مارك توسون، ترجمة د/ خالد العامري، التجارة الإلكترونية، دار الفاروق للنشر والتوزيع، القاهرة، الطبعة الأولى، عام 2000م.
- سايمون كولن، نقله إلى العربية، يحيى مصلح، التجارة على الإنترنت، بيت الأفكار الدولية بأمريكا، 1999م.
- د / محمد بن محمود مندورة، التخطيط للمجتمع المعلوماتي، جامعة الملك سعود، 1411هـ.
- د/ عبادة أحمد عبادة، مركز البحوث والدراسات، التدمير المتعمد لأنظمة المعلومات الإلكترونية، شرطة دبي بدولة الإمارات العربية المتحدة.

- د/ محمد القاسم، ود/ رشيد الزهراني، تشريعات تقنية المعلومات بالمملكة العربيـــة الســـعودية – الواقـــع والطموح والمعوقات، ورشة العمل الثالثة (أحكام في المعلوماتية)، 19/ شوال/ 1423هـ، الرياض.
- الدكتور/ عباس العبودي، التعاقد عن طريق وسائل الاتصال الفوري وحجيتها فـــي الإثبـــات، مكتبـــة دار الثقافة للنشر والتوزيع عمان، الأردن.
- د/ خالد بن محمد الطويل، مركز المعلومات الوطني، التعامل مع الاعتداءات الإلكترونيـــة مـــن الناحيـــة الأمنية، وزارة الداخلية، ورقة عمل مقدمة لورشة العمل الثالثة (أحكام في المعلوماتية) الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات 19 / 10 / 1423هـ الرياض.
- د/ مضر عدنان زهران، والمهندس/ عمر عدنان زهران، التعليم عن طريق الإنترنت، دار زهران للنشر، عمان، الأردن، عام 2002م.
- طوني ميشال عيسى، دار صادر بيروت، التنظيم القانوني لشبكة الإنترنـــت، لبنـــان، الطبعـــة الأولـــى، 2001م.
- د/ سهير حجازي، التهديدات الإجرامية للتجارة الإلكترونية، مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة.
- د/ أحمد شرف الدين، التوقيع الإلكتروني، مؤتمر التجارة الإلكترونية والإفلاس عبر الحـــدود، القـــاهرة، 2000م.
- د/ ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية (الجريمة عبـــر الإنترنـــت)، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، بجامعة الإمـــارات العربيـــة المتحدة، عام 2000م.
- دكتور/ مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنـــت، دار النهضـــة العربيـــة، القـــاهرة عام2000م.
- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2003م.
- د/ هشام محمد فريد رستم، الجرائم المعلوماتية (أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربيـــة موحدة للتدريب التخصصي)، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام 2000م.
- د/ إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعامل عبر وسائل الاتصال الحديثة، بحث مقـــدم إلـــى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، بجامعة الإمارات العربيـــة المتحـــدة، عـــام 2000م.
- الدكتور/ فتحي الدريني، حق الابتكار في الفقه الإسلامي، مؤسسة الرسالة، الطبعة الثالثة، 1404هـ.
- الدكتور/ فتحي الدريني، الحق ومدى سلطان الدولة في تقييده، جامعة دمشق، 1386هـ.

- د/ وهبة الزحيلي، حكم المصنفات الفنية (برامج الحاسوب)، دار المكتبي للطباعة والنشر، دمشق، سوريا الطبعة الأولى، 1418هـ.
- د/ أسامة قايد، الحماية الجنائية الخاصة، دار النهضة العربية، القاهرة، 1994م.
- د/ علي بن عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام 2000م.
- د/ مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، عام 2001م.
- د/ هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، عام 2000م.
- علي بن محمد السحيباني، و د/ عاصم بن محمد السعيد، حماية الحقوق الفكرية، سجل الملتقى العلمي حول حماية الحقوق الفكرية، الكلية التقنية بالرياض، 1420/11/16هـ
- د/ صالح بن عبد الله بن حميد، حماية الحقوق الفكرية من منظور إسلامي، بحث مقدم إلى ملتقى حماية الحقوق الفكرية المعقود بالكلية التقنية بالرياض 16 / 11 / 1420هـ.
- محمد بن عبد الله النافع، حماية الخصوصية للأفراد والجهات في ضوء الشريعة الإسلامية، بحث مقدم لورشة العمل الثالثة (أحكام في المعلوماتية) التي نظمها مشروع الخطة الوطنية لتقنية المعلومات 1423/10/19هـ، الرياض.
- د/ علي بن فايز الجحني، حماية الفكر وتحديات البحث العلمي، بحث مقدم إلى ملتقى حماية الحقوق الفكرية، المعقود بالكلية التقنية بالرياض في 16 / 11 / 1420هـ.
- د/ ناصر بن حمد القبيسي، ود/ عاصم بن محمد السعيد، الحماية الفكرية و وأثرها على الإبداع، بحث مقدم إلى ملتقى حماية الحقوق الفكرية، المنعقد بالكلية التقنية بالرياض في 1420/11/16هـ.
- د/ محمد محي الدين عوض، حماية الملكية الفكرية من الناحية القانونية، بحث مقدم إلى ملتقى حماية الحقوق الفكرية، المعقود بالكلية التقنية بالرياض في 16 / 11 / 1420هـ.
- عبيد الله بن محمد العبيد الله، حماية حقوق المؤلف في المملكة العربية السعودية، ضمن دورة حقوق الملكية الفكرية المعقودة بتاريخ 12 / 11 / 1422هـ بمركز الملك فيصل للبحوث والدراسات الإسلامية، معهد الفيصل لتنمية الموارد البشرية.
- د/ أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الإنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، الذي نظمته كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام 2000م.
- فريده كيت، الخصوصية في عصر المعلومات، ترجمة: محمد محمود شهاب، مركز الأهرام للترجمة والنشر القاهرة، الطبعة الأولى، 1420هـ.

- د/عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر 2000 م.
- د/ عادل محمود شرف، ود/ عبد الله إسماعيل عبد الله، ضمانات الأمن والتأمين في شبكة الإنترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانونية، بجامعة الإمارات العربية المتحدة، عام 2000م.
- دكتور/ فاروق محمد أحمد الأباصيري، العقود التجارية الإلكترونية، دار الجامعة الجديدة للنشر، 2002م.

المؤلفات الأجنبية:

- Alian Bensoussan: le commerce électronique, aspects Juridiques, Hermès, 1988.
- Bibent Michel: le droit du traitement de l'information, Nathan, 2000.
- Buffelan: les nouveaux délits informatiques expertise , 1988,
- Deveze (J.): Commentaire de la loi No. 88 – 19 du 5 Jan. 1988, relative a la Froude informatique, la droit de l'informatique 1987, mise a jour Février, 1988, No. 26
- Garsain (R.): informatique (Fraude informatique) Dalloz 1989.
- Fishnigni Deborah: National and international Aspects of computer crime , the emerging need for statutory controls , theses of , London , center for criminal law studies , Westfield , 1993.
- Lucas de Leyssac: Commentateur de la loi du 5 Jan. 1988 R.D, informatique télécom, 1988.
- Lucas Leyssac: Fraude informatique, loi du sjanvier 1988.
- Stepain , levaseur et Bouloc: Droit pénal général , 13 éd , 1987. No 279.
- Philippe Rose: La criminalité informatique, puff, 1 éd ,1988.
- Jérôme Huet et Herbert Maisi droit de l'informatique et des télécommunications de lois constitution.
- Vivant (M.) et Stanc (Ch.): la droit de le informatique , 1989.

المجلات العلمية:

- Amdre Lucas: le droit de l'informatique, P.U.F 1993.
- Barit (M.): le fraudé informatique , une approche de droit comparé,Rev.D.P.C,No.4 avril, 1985,
- Bain bridge David Hacking: The un authorized access of computer system , the legal implications , M.L.Rev.March 1989 ,Vol. 52
- Croze: l'apport du droit pénal 'a loi la théorie du la fraudé de l'informatique c'a propos de la loi no 88-19 du Janvier 1988 relative 'a la fraude informatique, J.C.P 1988 ,13,No.7
- Chamoux: la loi Sun la Froude informatique de nouvelles in criminalisons , J.C.P 1988. 13. No.7
- Michel Kreisler: l'investissement informatique de l'entreprise et sa protection pénal, G.P. 1990,P.6

- Devez: infraction en matière informatique, J.C.P 1988,
- Devez (J.): la fraudé informatique, aspects Juridiques, J.C.P 1987 – 1-3289
- LUCAS (A.): Le droit de l'informatique P.U.F. 1987.P.519. By.E.M: le financement de logiciels.GAZ.pal.1985.
- Hansen Ann C: Criminal law theft use of computer Services , state V. Megraw , W.E.l. rev.2007. vol. 7.
- Stravropolou Maria , Read chirs: computer crime The new Greek law, C.L.P. 1989.
- Silber Ulrich: computer crime and other crimes against information , I.R.P.L. 1993.Vol.64.
- Tiedeman: fraude et autres délits d'affaires commis 'a l'aide d'ordinateurs électroniques R.D.P.C 1984.
- Tappolet: la fraude informatique, Rêve. inter. Crim. et Pol. techn. 1988.
- Pradel (J.): les infractions relatives 'a L'informatique R.D.P.C, 1990.
- Pradel et feuillard: les infraction commise au moyen de l'ordinateur,R.Dr.pen.et crime 1985.